(2024) 25 SAL Ann Rev 270
(Published on e-First 30 April 2025)

11. CONFIDENTIAL INFORMATION AND DATA PROTECTION

Benjamin **WONG**
LLM (London School of Economics),
LLB (Hons) (National University of Singapore);
Advocate and Solicitor (Singapore);
Lecturer, Faculty of Law, National University of Singapore.

CONFIDENTIAL INFORMATION

I. Test for breach of confidence

11.1 The Court of Appeal delivered its decision in the case of *Lim Suk Ling Priscilla v Amber Compounding Pharmacy Pte Ltd*[1] on 20 May 2024.

11.2 This decision was primarily about the interaction between the traditional test for breach of confidence as set out in *Coco v A N Clark (Engineers) Ltd*[2] ("*Coco*") and the modified test for breach of confidence as set out in *I-Admin (Singapore) Pte Ltd v Hong Ying Ting*[3] ("*I-Admin*"). As background, under the traditional *Coco* test, the plaintiff must prove three elements: (a) "the information must possess the necessary quality of confidentiality"; (b) "the information must have been imparted in circumstances importing an obligation of confidence"; and (c) "there must be an unauthorised use of that information to the detriment of the party communicating it".[4] Under the modified *I-Admin* test, the plaintiff must prove the first two elements in the traditional *Coco* test, after which "an action for breach of confidence is presumed", and the defendant then has the burden of proving that his "conscience was unaffected" in order to rebut the presumption.[5] Conceptually, a claim under the traditional *Coco* test is for the "wrongful gain" of the defendant, while a claim under the modified *I-Admin* test is for the "wrongful loss" of the plaintiff.[6]

11.3 In this case, the respondents were Amber Compounding Pharmacy Pte Ltd and Amber Laboratories Pte Ltd, which were two companies in the business of pharmaceutical compounding. The

1 [2024] 1 SLR 741.
2 [1969] RPC 41.
3 [2020] 1 SLR 1130.
4 *Clearlab SG Pte Ltd v Ting Chong Chai* [2015] 1 SLR 163 at [64].
5 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [61].
6 *Lim Oon Kuin v Rajah & Tann Singapore LLP* [2022] 2 SLR 280 at [39].

appellants were Lim (who was an ex-employee of Amber Compounding Pharmacy Pte Ltd) and Compounding Pharmacy Pte Ltd (which was a company also in the business of pharmaceutical compounding, and was incorporated by Lim along with a partner). The respondents sued various defendants, including the appellants, for breach of confidence (among other things).

11.4 The parties eventually reached a settlement agreement, with the appellants entering into a consent judgment in which they admitted to their breach of confidence against the respondents. However, the parties were unable to agree on the specific issue of whether the respondents were entitled to "claim *both* traditional damages for wrongful gain under the principles laid down in [*Coco*] and equitable damages for wrongful loss under the principles laid down in [*I-Admin*]" in the same action [emphasis in original].[7] The General Division of the High Court answered this question (the "Narrow Issue") in the affirmative.[8] On the broader issue of whether the respondents were entitled to claim for both the wrongful gain interest and the wrongful loss interest *in respect of the same document* (the "Broad Issue"), the court declined to decide because the parties had not made arguments on the issue.[9]

11.5 The appellants appealed the decision of the General Division of the High Court. On appeal, the appellants argued that the Narrow Issue and Broad Issue should both be answered in the negative,[10] while the respondents argued that the Narrow Issue and the Broad Issue should both be answered in the affirmative.[11]

11.6 As a preliminary matter, the Court of Appeal highlighted that both the Narrow Issue and the Broad Issue were moot. This was because the consent judgment was predicated on the appellants' wrongful use of confidential information, and as a consequence the respondents could only claim damages under the traditional *Coco* test.[12] Accordingly, the court's opinions in this decision are necessarily in *obiter dicta*.

---

7 *Lim Suk Ling Priscilla v Amber Compounding Pharmacy Pte Ltd* [2024] 1 SLR 741 at [3].

8 *Amber Compounding Pharmacy Pte Ltd v Lim Suk Ling Priscilla* [2023] SGHC 241 at [16].

9 *Amber Compounding Pharmacy Pte Ltd v Lim Suk Ling Priscilla* [2023] SGHC 241 at [31].

10 *Lim Suk Ling Priscilla v Amber Compounding Pharmacy Pte Ltd* [2024] 1 SLR 741 at [21].

11 *Lim Suk Ling Priscilla v Amber Compounding Pharmacy Pte Ltd* [2024] 1 SLR 741 at [24].

12 *Lim Suk Ling Priscilla v Amber Compounding Pharmacy Pte Ltd* [2024] 1 SLR 741 at [6].

(cont'd on the next page)

11.7 The court held that the Narrow Issue should be answered in the affirmative (*ie*, the plaintiff can claim for both the wrongful loss interest and the wrongful gain interest in the same action), in so far as the claims for the wrongful loss interest and the claims for the wrongful gain interest are made in relation to different documents.[13] This is because an action for breach of confidence may involve multiple documents, and the claim must be assessed with reference to each document, such that it is possible that the traditional *Coco* test ought to be applied to some of the documents, while the modified *I-Admin* test ought to be applied to other documents.[14]

11.8 As for the Broad Issue, however, the court held that it should be answered in the negative (*ie*, the plaintiff cannot claim for both the wrongful loss interest and the wrongful gain interest in respect of the same document).[15] This is because the modified *I-Admin* test was meant to fill a lacuna in the law left by the traditional *Coco* test, which provided no remedy to plaintiffs whose confidential information was taken but not used; in a situation where the traditional *Coco* test did already provide a remedy, there was no lacuna for the modified *I-Admin* test to fill.[16] Further, under the traditional *Coco* test, damages included the loss of confidentiality of the confidential information, and allowing a separate claim under the modified *I-Admin* test could result in double recovery.[17] Finally, there would be "conflicting burdens of proof" if both tests were applied in respect of the same set of documents.[18] Nevertheless, while the plaintiff cannot plead both wrongful loss and wrongful gain in respect of the same set of documents, it is open to the plaintiff to plead wrongful loss as an alternative to a primary plea of wrongful gain.[19]

11.9 This case provides important and timely clarity by deconflicting the traditional *Coco* test and the modified *I-Admin* test. It is submitted that there will now be very little doubt as to the correct test to apply in a particular case.

---

13 *Lim Suk Ling Priscilla v Amber Compounding Pharmacy Pte Ltd* [2024] 1 SLR 741 at [42].
14 *Lim Suk Ling Priscilla v Amber Compounding Pharmacy Pte Ltd* [2024] 1 SLR 741 at [35]–[39].
15 *Lim Suk Ling Priscilla v Amber Compounding Pharmacy Pte Ltd* [2024] 1 SLR 741 at [48].
16 *Lim Suk Ling Priscilla v Amber Compounding Pharmacy Pte Ltd* [2024] 1 SLR 741 at [45].
17 *Lim Suk Ling Priscilla v Amber Compounding Pharmacy Pte Ltd* [2024] 1 SLR 741 at [46].
18 *Lim Suk Ling Priscilla v Amber Compounding Pharmacy Pte Ltd* [2024] 1 SLR 741 at [47].
19 *Lim Suk Ling Priscilla v Amber Compounding Pharmacy Pte Ltd* [2024] 1 SLR 741 at [49]–[50].

II. Account of profits and equitable damages

11.10 The General Division of the High Court delivered its decision in the case of *3D Infosystems Pte Ltd v Voon South Shiong*[20] on 16 September 2024.

11.11 In this case, the plaintiff ("3D Infosystems") was a company that provided IT services. The first defendant ("Voon") was a senior employee in 3D Infosystems before he left in 2018. The second defendant ("Sunway Digital") was a company that provided digital transformation services. Voon provided consultancy services to Sunway Digital through his own company ("JMPL") after he left the employment of 3D Infosystems.

11.12 In a previous judgment,[21] Voon and Sunway Digital had been held liable for various wrongs committed against 3D Infosystems. These wrongs included breaches of confidence committed by Voon. Voon's breaches of confidence consisted in his disclosure of 3D Infosystems' confidential information to Sunway Digital. The confidential information disclosed by Voon included client and financial information (contained in a business plan that Voon prepared for Sunway Digital), internal manuals and pricing strategies.[22]

11.13 The present case dealt with the assessment of damages to be paid to 3D Infosystems, including the damages to be paid for Voon's breaches of confidence. While the parties had agreed on the damages payable under many of the heads of claim, some heads of claim were disputed. In particular, there were four disputed heads of claim pertaining to Voon's breaches of confidence.

11.14 The first relevant disputed head of claim was for Voon's wrongful disclosure of 3D Infosystems' client and financial information in the business plan that Voon had prepared for Sunway Digital.[23] 3D Infosystems claimed an account of profits from Voon, as Sunway Digital had paid consultancy fees to JMPL. 3D Infosystems quantified its claim using the formula of A – B = C, where the components A, B, and C were described as follows:[24]

20 [2024] SGHC 237.
21 *3D Networks Singapore Pte Ltd v Voon South Shiong* [2023] 4 SLR 396.
22 *3D Networks Singapore Pte Ltd v Voon South Shiong* [2023] 4 SLR 396 at [151].
23 *3D Infosystems Pte Ltd v Voon South Shiong* [2024] SGHC 237 at [20].
24 *3D Infosystems Pte Ltd v Voon South Shiong* [2024] SGHC 237 at [21].

(a) Component A: amount of remuneration Voon received (through JMPL) from Sunway Digital.

(b) Component B: value of Voon's legitimate services provided to Sunway Digital.

(c) Component C: amount of Voon's remuneration attributable to Voon's breach (and thus subject to an account of profits).

11.15 In a claim for an account of profits, the plaintiff can only claim profits attributable to the defendant's breach, and cannot claim profits attributable to the defendant's legitimate work. Therefore, the plaintiff must isolate and quantify the portion of profits attributable to the defendant's breach. The court found that 3D Infosystems' formula was a "workable" way of doing so.[25]

11.16 The court acknowledged that the process of quantification would involve the making of "assumptions" and "educated guesses", and that "the court will simply do the best that it can".[26] Component A was assessed to be $898,300. This amount was based on the monthly consultancy fees paid by Sunway Digital to JMPL within the relevant period.[27] Component B was assessed to be $712,395.83. This was done using a salary guide published by Morgan McKinley to benchmark the value of Voon's services, assigning a value to each component of Voon's services by pro-rating the corresponding salary indicators.[28] Component C, being the remainder after Component B was deducted from Component A, was accordingly assessed to be $185,904.17 – this was the amount of profits attributable to Voon's breach of confidence, which had to be disgorged by Voon.[29]

11.17 The second relevant disputed head of claim was for Voon's wrongful disclosure of 3D Infosystems' internal manuals to Sunway Digital. 3D Infosystems sought equitable damages (amounting to $25,612.06) based on the value of the confidential information in the internal manuals. 3D Infosystems relied on the Court of Appeal's decision in *I-Admin*, wherein the court had ordered equitable damages to be assessed against the defendants based on the value of the confidential information that they had taken.[30] As for how the value of the confidential information was to be assessed, 3D Infosystems adopted the "cost savings" approach

25 *3D Infosystems Pte Ltd v Voon South Shiong* [2024] SGHC 237 at [23].
26 *3D Infosystems Pte Ltd v Voon South Shiong* [2024] SGHC 237 at [24].
27 *3D Infosystems Pte Ltd v Voon South Shiong* [2024] SGHC 237 at [25]–[32].
28 *3D Infosystems Pte Ltd v Voon South Shiong* [2024] SGHC 237 at [33]–[39].
29 *3D Infosystems Pte Ltd v Voon South Shiong* [2024] SGHC 237 at [40].
30 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [78]–[79].

taken by the court in *I-Admin*: the value of the confidential information was the costs saved by Sunway Digital by not having to independently develop the internal manuals, and these costs were themselves measured by the costs that 3D Infosystems itself incurred when developing the internal manuals.[31] However, the court rejected 3D Infosystems' claim for equitable damages because 3D Infosystems had not proved that Sunway Digital had actually used the confidential information.[32] According to the court, the *I-Admin* "cost savings" approach of assessing equitable damages was only applicable if the defendant had actually used the confidential information – for if the defendant had not actually used the confidential information, then it would not have enjoyed any cost savings.[33]

11.18 The third and fourth relevant disputed heads of claim were for Voon's wrongful disclosure of 3D Infosystems' pricing strategy for its bids for two separate projects (namely, the "SCADA 227 Project" and the "OEM2 Project"). In both cases, 3D Infosystems alleged that the disclosure of its pricing strategies caused it to lose its bids for the projects, as Sunway Digital had used its knowledge of the pricing strategies to undercut 3D Infosystems' bids. 3D Infosystems sought damages for its resultant losses of profits. In relation to the SCADA 227 Project, 3D Infosystems succeeded in its claim, and was awarded $269,509.87 (being the estimated profit margin it would have obtained from the project).[34] In relation to the OEM2 Project, however, 3D Infosystems failed in its claim because it had failed to prove causation (*ie*, it had failed to prove that, but for the breach, it would have won the bid for the OEM2 Project).[35]

11.19 This case is principally notable for two points relating to damages for breach of confidence.

11.20 The first point pertains to account of profits for breach of confidence. When assessing the quantum of profits to be disgorged, only profits that are "caused by" (or attributable to) the breach of confidence are liable to be disgorged. In cases where a part of the profits is not attributable to the breach of confidence, it can be difficult to isolate and quantify the part of the profits that is attributable to the breach of confidence. One solution that was applied in this case is to subtract away those parts of the profits that are *not* attributable to the breach of confidence from the total profits, and regard the remainder as the profits that are attributable to the breach of confidence.

---

31 *3D Infosystems Pte Ltd v Voon South Shiong* [2024] SGHC 237 at [91].
32 *3D Infosystems Pte Ltd v Voon South Shiong* [2024] SGHC 237 at [94].
33 *3D Infosystems Pte Ltd v Voon South Shiong* [2024] SGHC 237 at [95].
34 *3D Infosystems Pte Ltd v Voon South Shiong* [2024] SGHC 237 at [132].
35 *3D Infosystems Pte Ltd v Voon South Shiong* [2024] SGHC 237 at [141].

11.21 The second point pertains to equitable damages for breach of confidence. This case clarifies that, if a plaintiff wishes to claim equitable damages based on the *I-Admin* "cost savings" approach, the plaintiff must prove that the defendant had used the confidential information (and thereby saved costs). However, it should also be noted that the *I-Admin* "cost savings" approach may not be the only way to assess equitable damages for breach of confidence, as there may be other methods of assessing the value of confidential information in a particular case (*eg*, by valuing the confidential information by reference to its market price).

III. Retention of confidential information

11.22 The Court of Appeal delivered its decision in the case of *Syed Suhail bin Syed Zin v Attorney-General*[36] on 11 October 2024.

11.23 The appellants in this case were 13 individuals who had been prisoners in Changi Prison. The respondent was the Attorney-General ("AG").

11.24 The Singapore Prison Services ("SPS") had disclosed correspondence belonging to the appellants to the Attorney-General's Chambers ("AGC"). The appellants commenced proceedings against the AG, seeking (among other things) a declaration that the "AG committed a breach of confidence by the disclosure and retention of confidential correspondence" belonging to the prisoners, as well as an "order for damages and/or equitable relief … for breach of confidence".[37]

11.25 The General Division of the High Court dismissed the appellants' claims. In relation to the claim for breach of confidence, the judge applied the modified test for breach of confidence as set out in *I-Admin*, and held that there was "no actionable breach of confidence" on the facts of the case, because although there was a presumed breach of confidence by the AG, this presumption was rebutted as the AG's conscience was unaffected.[38] The appellants appealed this decision.

11.26 The Court of Appeal reversed the decision of the General Division of the High Court on the issue of breach of confidence, and made a declaration that the AG had committed a breach of confidence against all but two of the prisoners by disclosing and retaining confidential information belonging to them.[39] Here, the court applied the modified

36 [2024] 2 SLR 588.
37 *Syed Suhail bin Syed Zin v Attorney-General* [2024] 2 SLR 588 at [7].
38 *Syed Suhail bin Syed Zin v Attorney-General* [2024] 2 SLR 588 at [15].
39 *Syed Suhail bin Syed Zin v Attorney-General* [2024] 2 SLR 588 at [63].

I-Admin test for breach of confidence.[40] The court began by determining which letters were confidential, and found that some letters that were written to or received from certain public institutions (such as the Supreme Court and the Singapore Police Force) were not confidential, while other letters that were subject to privilege were confidential.[41] Next, the court found that the consciences of both the AGC and the SPS were affected by the disclosure and retention of the confidential letters, as both the AGC and the SPS must be taken to have known that the letters were confidential.[42]

11.27 However, the court declined to award damages to the prisoners whose right to confidentiality had been breached. The court began by noting that only equitable remedies were available for breach of confidence, and these remedies were awarded at the court's discretion, with the plaintiffs bearing the burden of proving that they were entitled to these remedies.[43] In relation to the prisoners' claim for punitive damages, the court found that the prisoners had not provided any legal basis for extending punitive damages to breaches of confidence, and that the prisoners had in any case failed to claim for punitive damages in their originating summons.[44] The court also considered whether the remedies of account of profits, equitable compensation, and equitable remedies were available, and found that there was no basis for any of these remedies.[45] Finally, the court rejected the prisoners' claim for damages "in respect of criminal proceedings which had been unfairly tainted by disclosure of their correspondence".[46]

11.28 What is of interest in this case is how the court dealt with the retention of confidential information by the defendant (namely, the AG). Here, the court found that the AG had committed a breach of confidence based on the *I-Admin* modified test for breach of confidence. This provides clarity on two matters. First, while the Court of Appeal had in previous cases already confirmed that the *I-Admin* test ought properly to apply to cases where the defendant is alleged to have wrongfully acquired the plaintiff's confidential information, this case clarifies that the application of the *I-Admin* test extends to cases where the allegation is that the defendant had passively received the confidential information and then retained it. Second, this case also clarifies that the retention of confidential information can amount to a breach of confidence under the

40 *Syed Suhail bin Syed Zin v Attorney-General* [2024] 2 SLR 588 at [50].
41 *Syed Suhail bin Syed Zin v Attorney-General* [2024] 2 SLR 588 at [54]–[61].
42 *Syed Suhail bin Syed Zin v Attorney-General* [2024] 2 SLR 588 at [62].
43 *Syed Suhail bin Syed Zin v Attorney-General* [2024] 2 SLR 588 at [64].
44 *Syed Suhail bin Syed Zin v Attorney-General* [2024] 2 SLR 588 at [70]–[74].
45 *Syed Suhail bin Syed Zin v Attorney-General* [2024] 2 SLR 588 at [75]–[76].
46 *Syed Suhail bin Syed Zin v Attorney-General* [2024] 2 SLR 588 at [66]–[69].

I-Admin test – indeed, the court explicitly held that the mere retention of documents could amount to a breach of confidence.[47] That said, it is likely that the retention of documents will only amount to a breach of confidence if the defendant knew that the documents contained information of a confidential nature, as the defendant's lack of knowledge about the confidential nature of the information is likely to mean that the defendant's conscience was unaffected.[48]

DATA PROTECTION

IV. Data minimisation, personal data inventory and data breach notification

11.29 The Personal Data Protection Commission ("PDPC") delivered its decision in the case of *Re Keppel Telecommunications & Transportation Ltd*[49] on 14 May 2024.

11.30 This case involved two organisations, namely Geodis Logistics Singapore Pte Ltd ("GLS") and Keppel Telecommunications & Transportation Ltd ("KTT"). GLS was a wholly-owned subsidiary of KTT.

11.31 Both organisations shared a server belonging to GLS. On this server, the organisations stored personal data of various individuals – these individuals included the employees, directors, and shareholders of the organisations and their affiliates.

11.32 In May 2020, KTT migrated its data (including the personal data) from the server to cloud storage. However, KTT omitted to instruct its staff to delete the personal data from the server after the migration. As a result, a copy of the personal data remained on the server after the migration. GLS continued to use the server for its own operations.

11.33 In July 2022, KTT divested GLS. Before the divestment, KTT reminded its staff to transfer any files stored on the server to cloud storage. However, KTT again omitted to instruct its staff to delete the files on the server after transferring the files to cloud storage.

11.34 Subsequently, it was discovered that an unknown attacker had accessed multiple files on the server in September 2022. There was

47 *Syed Suhail bin Syed Zin v Attorney-General* [2024] 2 SLR 588 at [62].
48 See *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [61].
49 [2024] SGPDPC 3.

also a distinct possibility that some of the files on the server had been exfiltrated and published on the dark web.

11.35 KTT and GLS notified the PDPC about the data breach. The PDPC then commenced investigations against the organisations for potential breaches of the Personal Data Protection Act 2012[50] ("PDPA"). However, as GLS gave a voluntary undertaking which was accepted by the PDPC, the PDPC took no further action against GLS.

11.36 Pursuant to its investigation, the PDPC found that KTT had breached the Protection Obligation under s 24 of the PDPA.[51] KTT breached the Protection Obligation by failing to ensure the deletion of the personal data stored on the server after the migration of the data to cloud storage.[52] The PDPC ordered KTT to pay a financial penalty of $120,000.[53]

11.37 Three useful points may be drawn from this case.

11.38 First, this case demonstrates the importance of data minimisation. In particular, it shows that organisations should not retain unnecessary personal data, and that the unnecessary retention of personal data can constitute a breach of the Protection Obligation. As stated by the PDPC in its decision, organisations should dispose of personal data that is no longer needed.[54] In this case, KTT ought to have deleted the personal data on the server after migrating its data to cloud storage, since it was no longer necessary to have a copy of the personal data on the server. KTT's failure to do so was a breach of the Protection Obligation. Arguably, if KTT had properly deleted the personal data on the server after migrating its data to cloud storage, the data breach would not have occurred since there would have been no personal data on the server for the unknown attacker to access.

11.39 Second, this case also demonstrates the utility of maintaining a comprehensive personal data asset inventory. As noted by the PDPC in its decision, "[t]he creation and maintenance of a personal data asset inventory is an established security practice" which enables an organisation to keep track of its personal data.[55] In this case, if KTT had maintained a comprehensive personal data asset inventory, then it would have been less likely for KTT to have overlooked the existence

50 2020 Rev Ed.
51 *Re Keppel Telecommunications & Transportation Ltd* [2024] SGPDPC 3 at [29].
52 *Re Keppel Telecommunications & Transportation Ltd* [2024] SGPDPC 3 at [28].
53 *Re Keppel Telecommunications & Transportation Ltd* [2024] SGPDPC 3 at [41].
54 *Re Keppel Telecommunications & Transportation Ltd* [2024] SGPDPC 3 at [25].
55 *Re Keppel Telecommunications & Transportation Ltd* [2024] SGPDPC 3 at [31].

of the personal data on the server (an oversight which KTT admitted to committing),[56] and it would have been more likely that KTT would remember to instruct its staff to delete the personal data from the server. That being said, the PDPC emphasised that its comments about personal data asset inventories were "solely to provide guidance" and did not factor into its decision on the breach of the Protection Obligation by KTT.[57]

11.40 Third, it is interesting to note that the PDPC partially waived the requirement for KTT to make a data breach notification to the affected individuals. Under the Data Breach Notification Obligation of the PDPA, organisations are required to notify individuals of data breaches affecting them, under certain circumstances.[58] Ostensibly, this was a case in which a data breach notification was required of KTT.[59] However, the PDPC has the statutory power to waive this requirement.[60] In this case, the PDPC granted KTT a waiver in respect of certain overseas-based affected individuals "whose contact information [KTT] did not have and could not obtain after making reasonable enquiries".[61] In future, it may be possible for other organisations in similar circumstances to apply for and obtain a limited waiver of this kind.

V. Deemed consent, exceptions to consent and right of private action

11.41 The District Court delivered its decision in the case of *Martin Piper v Singapore Kindness Movement*[62] on 12 November 2024.

11.42 On 27 August 2022, the plaintiff ("Piper") sent an e-mail ("27 August E-mail") to the defendant ("SKM"), in order to complain about the conduct of Loi, who was the co-founder of an organisation affiliated with SKM. On 1 September 2022, the deputy director of SKM ("Karun") replied by e-mail ("1 September E-mail") to Piper to inform him that he had contacted Loi, and conveyed Loi's response to Piper's complaint. Karun also told Piper that he could contact Loi directly for further clarification. On 4 September 2022, Piper replied with two e-mails to Karun with more information about Loi's conduct. Finally, on 7 September 2022, Karun sent Loi an e-mail (with Piper copied in) which set out the chain of e-mail correspondence between Piper and Karun, and

56 *Re Keppel Telecommunications & Transportation Ltd* [2024] SGPDPC 3 at [11]–[12].
57 *Re Keppel Telecommunications & Transportation Ltd* [2024] SGPDPC 3 at [30].
58 Personal Data Protection Act 2012 (2020 Rev Ed) s 26D(2).
59 *Re Keppel Telecommunications & Transportation Ltd* [2024] SGPDPC 3 at [21]–[22].
60 Personal Data Protection Act 2012 (2020 Rev Ed) s 26D(7).
61 *Re Keppel Telecommunications & Transportation Ltd* [2024] SGPDPC 3 at [20].
62 [2024] SGDC 292.

in which Karun stated that it would be best for Loi to respond directly to Piper.

11.43 Piper brought a claim against SKM pursuant to the right of private action under s 48O of the PDPA, alleging that SKM had breached its obligations under the PDPA by sending the 7 September e-mail to Loi, as SKM had thereby disclosed Piper's personal data to Loi as Loi could see the e-mail correspondence between Piper and Karun.

11.44 In his closing submissions at trial, Piper included three additional instances of disclosure of his personal data in his claim against SKM, which became known during the course of the trial. First, the general secretary of SKM ("Dr Wan") had disclosed Piper's identity to Loi in a phone call on 30 August 2022. Second, Dr Wan again disclosed Piper's identity to Loi in a meeting with her and Karun to discuss the 27 August E-mail. Third, Karun had blindly copied Loi in the 1 September E-mail to Piper, which effectively disclosed Piper's name and e-mail address to Loi.

11.45 There were two issues in this case. The first issue was whether SKM had, by disclosing Piper's personal data to Loi, breached its obligations under the PDPA (in particular, the Consent Obligation, the Purpose Limitation Obligation, and the Notification Obligation). The second issue was whether Piper had suffered financial losses or emotional distress directly as a result of SKM's alleged breaches of the PDPA.

11.46 The court held that SKM had not breached the Consent Obligation. While it was true that SKM had not obtained express consent from Piper to disclose his personal data to Loi,[63] Piper should be deemed to have consented to the disclosure.[64] Section 15(1) of the PDPA provides that "[a]n individual is deemed to consent to the collection, use or disclosure of personal data about the individual by an organisation for a purpose" if the individual "voluntarily provides the personal data to the organisation for that purpose" and "it is reasonable that the individual would voluntarily provide the data". Here, Piper had provided his personal data to SKM for the purpose of SKM acting on his complaint against Loi, and it was reasonable that he would voluntarily provide his personal data for that purpose.[65] Although Piper argued that there was no need to disclose his personal data when acting on his complaint, the court found that SKM had acted reasonably in disclosing Piper's personal data, because the disclosure was the "most effective way" for SKM to act on Piper's complaint, and it was reasonable for SKM to expect Piper

63 *Martin Piper v Singapore Kindness Movement* [2024] SGDC 292 at [24].
64 *Martin Piper v Singapore Kindness Movement* [2024] SGDC 292 at [38].
65 *Martin Piper v Singapore Kindness Movement* [2024] SGDC 292 at [37].

to request anonymity if that was what he desired.[66] While Piper could have overridden this deemed consent by expressly requesting the non-disclosure of his personal data, he did not do so.[67]

11.47 Since there was deemed consent on the facts, SKM also did not breach the Notification Obligation, since an organisation need not give notice of its purposes to the individual when the individual is deemed to have consented to the disclosure of his personal data.[68] This is the effect of s 20(3)(*a*) of the PDPA. Further, the court also held that SKM did not breach the Purpose Limitation Obligation, as a "reasonable person would deem it appropriate in the circumstances to disclose [Piper's] identity in the course of investigating his complaint".[69]

11.48 For completeness, the court considered SKM's argument that two of the exceptions to the Consent Obligation were applicable in the present case. First, SKM argued that the "Individual's Interests Exception" was applicable. This exception is found in para 1(1) of Pt 1 of the First Schedule to the PDPA, which provides that consent is not required where "the collection, use or disclosure (as the case may be) of personal data about an individual is necessary for any purpose which is clearly in the individual's interests" and (a) "consent for the collection, use or disclosure (as the case may be) cannot be obtained in a timely way", or (b) "the individual would not reasonably be expected to withhold consent". SKM pleaded that para 1(1)(*b*) was applicable, on the basis that the disclosure of Piper's personal data was necessary to investigate his complaint which was clearly in his interests.[70] However, the court held that this exception was inapplicable because the word "interests" in this exception "appears to refer to matters of an urgent nature affecting the life, health or safety of an individual".[71]

11.49 Second, SKM argued that the "Investigation and Proceedings Exception" was applicable. This exception is found in para 3 of Pt 3 of the First Schedule to the PDPA, which provides that consent is not required where "[t]he collection, use or disclosure (as the case may be) of personal data about an individual is necessary for any investigation or proceedings". SKM pleaded that this exception was also applicable because the disclosure of Piper's personal data was necessary for investigating his complaint. However, the court found that this exception was inapplicable as the term "investigation" only covered investigations "relating to an

66 *Martin Piper v Singapore Kindness Movement* [2024] SGDC 292 at [39]–[44].
67 *Martin Piper v Singapore Kindness Movement* [2024] SGDC 292 at [45].
68 *Martin Piper v Singapore Kindness Movement* [2024] SGDC 292 at [51].
69 *Martin Piper v Singapore Kindness Movement* [2024] SGDC 292 at [53].
70 *Martin Piper v Singapore Kindness Movement* [2024] SGDC 292 at [58].
71 *Martin Piper v Singapore Kindness Movement* [2024] SGDC 292 at [60].

identified and specified wrong that is actionable in law", which did not describe the investigation in the present case.[72]

11.50 The court then dealt with the question of whether Piper had standing to sue under s 48O of the PDPA. Section 48O of the PDPA confers standing on an individual to sue for a breach of the PDPA, but only if the individual suffered "loss or damage directly as a result of" the breach. Piper alleged that he had suffered loss or damage because Loi filed an action under the Protection from Harassment Act 2014 against Piper, claiming that Piper's 27 August E-mail constituted harassment.[73] Further, Loi had published information about her claim on Facebook, leading to Piper receiving death threats.[74] As a result, Piper had to incur expense in defending against the claim, and also suffered emotional distress.[75] Further, Piper claimed that SKM was "dismissive" when responding to Piper's request for an explanation for its disclosure of his personal data to Loi, as SKM failed to reply in a timely manner.[76] However, the court held that any loss or damage suffered by Piper was not directly caused by SKM's disclosure of his personal data, but rather by Loi's claim against him and her publicising of her claim on Facebook.[77]

11.51 In addition, the court found that Piper did not actually suffer emotional distress, applying the multifactorial approach set out by the Court of Appeal in the case of *Reed, Michael v Bellingham, Alex*.[78] On the first factor of the nature of the personal data involved, the personal data was the identity of Piper; on the second factor of the nature of the breach, the breach was a one-off incident; on the third factor of the nature of the defendant's conduct, Piper had not alleged any "fraudulent or malicious intent" on the part of SKM; on the fourth factor of the risk of future breaches, the court found that this factor was entirely inapplicable to the case at hand; and on the fifth factor of the actual impact of the breach, Piper had not provided adequate evidence of his emotional distress stemming from SKM's breach.[79]

11.52 Three observations may be made about this case.

11.53 First, on deemed consent by voluntary provision of personal data, this case clarifies that, when an individual voluntarily provides his

72 *Martin Piper v Singapore Kindness Movement* [2024] SGDC 292 at [64].
73 *Martin Piper v Singapore Kindness Movement* [2024] SGDC 292 at [75].
74 *Martin Piper v Singapore Kindness Movement* [2024] SGDC 292 at [76].
75 *Martin Piper v Singapore Kindness Movement* [2024] SGDC 292 at [77].
76 *Martin Piper v Singapore Kindness Movement* [2024] SGDC 292 at [78].
77 *Martin Piper v Singapore Kindness Movement* [2024] SGDC 292 at [91]–[102].
78 [2022] 2 SLR 1156.
79 *Martin Piper v Singapore Kindness Movement* [2024] SGDC 292 at [111].

personal data to an organisation for a purpose, he may expressly limit the organisation's collection, use, or disclosure of his personal data. By doing so, he limits the scope of his deemed consent to the organisation's collection, use, or disclosure of his personal data for that purpose. In this case, the court made it clear that it was open to Piper to "expressly state that he did not want his identity to be disclosed".[80] Presumably, had Piper done so, he would not have been deemed to have consented to SKM's disclosure of his personal data to Loi.

11.54 Second, on exceptions to the Consent Obligation, the court provided important clarifications on the scopes of two exceptions, namely the Individual's Interests Exception and the Investigation and Proceedings Exception. Both of these exceptions were (correctly) given narrow interpretations.

11.55 Third, on the right of private action, this case makes it clear that an individual only has standing to sue if the organisation's breach of the PDPA *directly* caused loss or damage to him, and this requirement of directness is a strict one. As mentioned by the court, the "direct causal requirement in s 48O is to be stringently applied", as a control mechanism limiting the private liability of organisations under the PDPA.[81] If the individual's loss or damage is only indirectly caused by the organisation's breach, with an intervening event as the direct cause of the loss or damage, then the individual does not have standing to sue. The strictness of the direct causal requirement has the effect of severely limiting the ability of individuals to sue for breaches of the PDPA. It may also lead to surprising outcomes. For example, consider a hypothetical Organisation A with lax data security practices – this constitutes a breach of the Protection Obligation (which requires organisations to make reasonable security arrangements to protect personal data), but it is unlikely that such a breach would directly cause any loss or damage to the individuals whose personal data is held by Organisation A, and these individuals would therefore not have standing to sue Organisation A. Then, imagine that, as a result of Organisation A's lax data security practices, a malicious actor exfiltrates personal data from Organisation A's servers, and publishes it online, thereby causing emotional distress and other risks to the individuals concerned. In this scenario, it would appear that the individuals would still have no standing to sue Organisation A since the losses and damage caused to the individuals was only indirectly caused by Organisation A's lax data security practices.

80 *Martin Piper v Singapore Kindness Movement* [2024] SGDC 292 at [42].
81 *Martin Piper v Singapore Kindness Movement* [2024] SGDC 292 at [89].

11.56 In addition, what remains uncertain is whether an individual who has standing to sue (because the organisation's breach directly caused some loss or damage to him) can obtain remedies in respect of other loss or damage that was indirectly caused by the organisation's breach. Consider, for example, a scenario where Organisation A disclosed sensitive personal data of Person B to Person C. This disclosure was done without the consent of Person B and was thus a breach of the Consent Obligation. Person B, knowing of the disclosure and fearing that Person C would use the information to damage his reputation, suffered emotional distress. In this scenario, it is clear that Person B has standing to sue Organisation A for breach of the Consent Obligation. However, assume further that Person C subsequently did publish the sensitive personal data, causing Person B to lose his job – can Person B claim damages for his resultant financial loss when suing Organisation A, notwithstanding the fact that this financial loss was not directly caused by Organisation A's disclosure?