(2022) 34 SAcLJ 672
(Published on e-First 15 August 2022)

CLAIMING FOR BREACH OF CONFIDENCE AFTER A CYBERATTACK

Darren Lee Warren v DSG Retail Limited [2021] EWHC 2168 (QB)

In *Darren Lee Warren v DSG Retail Limited* [2021] EWHC 2168 (QB), the English High Court struck out Darren Lee Warren's claim against DSG Retail Limited for breach of confidence after the latter suffered a cyberattack which compromised the claimant's personal data. In doing so, the High Court found that it was clear that the claimant did not allege any positive conduct by the defendant said to constitute a breach of confidence, and his claim was in fact that the defendant failed in its alleged duties to provide sufficient security for his data. Since the cause of action in breach of confidence imposed a negative obligation not to disclose confidential information, and did not impose a data security duty, it had no realistic prospect of success. This case note argues that the decision of the English High Court to strike out the claim in breach of confidence was correct, and that the same outcome should be reached should a similar claim be brought in Singapore.

CHUA Ying-Hong[1]
LLB (First Class) (National University of Singapore), LLM (First Class) (University of Cambridge);
Advocate & Solicitor (Singapore).

I. Introduction

1 What recourse does a data subject have when his personal data is accessed or stolen in a cyberattack? Specifically, can he claim against the organisation whose systems were hacked (hereinafter referred to as the "data controller") for breach of confidence? Recourse against the data controller is important because the cyberattacker is often located outside the jurisdiction,[2] if he is even able to be identified at all. Specifically, a claim in breach of confidence against the data controller is important

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

2 See, for example, *Tucci v Peoples Trust Company* [2020] BCCA 246, where the cyberattacker was allegedly located in the People's Republic of China.

because the data subject may not have a contractual relationship with the data controller, so as to be able to claim in contract.

2 This case note examines the recent decision of the English High Court in *Darren Lee Warren v DSG Retail Limited*[3] ("*Warren v DSG*"), in which the claimant-data subject unsuccessfully claimed against the defendant-data controller for breach of confidence following a cyberattack which compromised his personal data. The English High Court found the breach of confidence claim to have no realistic prospect of success and struck it out. It is respectfully submitted that this outcome was correct. In fact, the same outcome should be reached in Singapore should a similar case arise, despite the recent expansion of the scope of breach of confidence claims in *I-Admin (Singapore) Pte Ltd v Hong Ying Ting*[4] ("*I-Admin*").

II. The decision of the English High Court in *Darren Lee Warren v DSG Retail Limited*

3 The key facts of *Warren v DSG* are as follows. The defendant, DSG Retail Limited ("DSG"), was a retailer operating the "Currys PC World" and "Dixons Travel" brands. It suffered a complex cyberattack carried out by "sophisticated and methodical criminals".[5] The attackers infiltrated DSG's systems and installed malware on close to 6,000 point-of-sale terminals at DSG's stores. In the course of the attack, the attackers accessed the personal data of many of DSG's customers.

4 The claimant, Darren Lee Warren, had purchased goods from Currys PC World. He claimed that his personal information, namely, his name, address, phone number, date of birth and email address, was compromised in the attack. He brought a claim in breach of confidence, misuse of private information, breach of the Data Protection Act 1998 and common law negligence against DSG. Specifically, he claimed damages of £5,000 for the distress he suffered as a result of his personal data being compromised and lost.

5 DSG applied for summary judgment and/or an order striking out each of the claims, except for the claim for breach of statutory duty arising out of the alleged breach of the seventh data protection principle ("DPP7"). DPP7 required "appropriate technical and organisational

3 [2021] EWHC 2168 (QB).
4 [2020] 1 SLR 1130.
5 *Darren Lee Warren v DSG Retail Limited* [2021] EWHC 2168 (QB) at [1].

measures to be taken against unauthorised or unlawful processing of data".

6 DSG argued that both the claims in breach of confidence and misuse of private information required the defendant to have taken some positive wrongful action in relation to the information in question, but DSG did not itself take any such positive wrongful action. Counsel for the claimant conceded that the breach of confidence claim was not tenable, but did not formally discontinue the claim. Counsel maintained that his case on misuse of private information had real prospects of success. Counsel emphasised the Information Commissioner's conclusion that DSG's culpability was "striking", and that it had knowledge of some deficiencies from 2014 and others from on or around May 2017. It was thus argued that DSG had intentionally and recklessly left the claimant's private information exposed to a real risk of intrusion and/or tantamount to publication to the world.

7 The High Court found that it was clear that the claimant did not allege any positive conduct by DSG said to comprise a breach or misuse for the purposes of either the breach of confidence or misuse of private information claim. This was unsurprising, since DSG was the victim of the cyberattack.[6] Rather, the claim was that DSG failed in alleged duties to provide sufficient security for the claimant's data. However, "neither BoC nor MPI impose a data security duty on the holders of information … Both are concerned with prohibiting actions by the holder of information which are inconsistent with the obligation of confidence/privacy".[7] Ultimately, the court stressed that "it was not DSG that disclosed the Claimant's personal data, or misused it, but the criminal third-party hackers".[8] The court thus struck out the claim in breach of confidence.

8 For completeness, it should be noted that the High Court's analysis is consistent with the line of English cases which established that it is not necessary to show that the defendant either deliberately or dishonestly misused confidential information in order to establish a claim in breach of confidence. As stated in *Gurry on Breach of Confidence*[9] ("*Gurry*"), the duty is broken simply by an unauthorised use or disclosure of the information, and the state of mind of the confidant in so misusing the information is irrelevant. For example, in *Seager v Copydex Ltd*,[10] the defendant was found liable in breach of confidence

6 *Darren Lee Warren v DSG Retail Limited* [2021] EWHC 2168 (QB) at [21].
7 *Darren Lee Warren v DSG Retail Limited* [2021] EWHC 2168 (QB) at [22].
8 *Darren Lee Warren v DSG Retail Limited* [2021] EWHC 2168 (QB) at [31].
9 Tanya Aplin *et al*, *Gurry on Breach of Confidence: The Protection of Confidential Information* (Oxford University Press, 2nd Ed, 2012) at para 15.32.
10 [1967] 1 WLR 923.

for having unconsciously made use of confidential information shared by the plaintiff about a carpet grip design in coming up with its own carpet grip. The plaintiff had invented and patented a carpet grip which the defendant was keen to market. During negotiations, the plaintiff revealed an alternative design for a carpet grip. After the negotiations fell through, the defendant developed its own carpet grip, which embodied the alternative idea which the plaintiff had earlier shared, and even used the name which the plaintiff allegedly mentioned. The Court found that the defendant honestly believed that the alternative design was its own idea, but it must have unconsciously made use of the information the plaintiff had provided earlier – the coincidences were too strong to permit of any other explanation. The Court of Appeal thus gave judgment for the plaintiff, with damages to be assessed.[11]

9 This principle, that a subconscious use of information obtained in confidence as a springboard for activities detrimental to the person who made the confidential communication may give rise to a claim for breach of confidence, was recently affirmed by the Privy Council in *Paymaster (Jamaica) Ltd v Grace Kennedy Remittance Services Ltd*,[12] citing *Seager v Copydex*. The Privy Council noted that conscious plagiarism is not a necessary component of the claim.

10 However, in the above line of cases, the defendant had in fact misused the plaintiff's confidential information. The only issue was whether the misuse was committed consciously. This may be contrasted with the situation in *Vestergaard Frandsen A/S v Bestnet Europe Limited*[13] ("*Vestergaard v Bestnet*"). Vestergaard developed and sold insecticidal bed nets. One of the defendants, Mrs Sig, was initially employed by Vestergaard. She later started a new business with another former Vestergaard employee manufacturing and selling insecticidal bed nets. They engaged one Dr Skovmand, who had developed Vestergaards' bed nets, to develop a new insecticidal bed net (Netprotect) for their new business. Vestergaard learnt of their new business and issued proceedings alleging breach of its trade secrets. At trial, Arnold J held that Mrs Sig was liable in breach of confidence. Counsel submitted that Mrs Sig could not be liable for breach of confidence absent a finding that she knew that the initial Netprotect recipes were derived from Vestergaard's confidential database. Arnold J disagreed and, citing *Seager v Copydex*, reiterated that a person could be liable for breach of confidence even if he was

11 The Appeal Committee of the House of Lords later dismissed the defendant's petition for leave to appeal.
12 [2018] Bus LR 492.
13 [2013] UKSC 31.

not conscious of the fact that what he was doing amounted to misuse of confidential information.

11 On appeal to the Court of Appeal, Jacob LJ said that *Seager v Copydex* was distinguishable because the defendants there were actually using the information which had been imparted to them, albeit unconsciously. This was not the case for Mrs Sig.

12 The Supreme Court agreed that Vestergaard's claim against Mrs Sig must fail because of two crucial facts. The first was that she did not ever acquire the confidential information in question, whether during the time of her employment with Vestergaard or afterwards. The second crucial fact was that Mrs Sig was unaware that the Netprotect product had been developed using Vestergaard's trade secrets until sometime during the legal proceedings. The Supreme Court held that the absence of such knowledge would appear to preclude liability, at least without the existence of special facts, as "[a]fter all, an action in breach of confidence is based ultimately on conscience". It was not contended that Mrs Sig could be vicariously liable for any misuse of Vestergaard's confidential information by Dr Skovmand (unsurprisingly, as Dr Skovmand worked for the new business, as did Mrs Sig). The Supreme Court held that, while a recipient of confidential information might be said to be primarily liable in a case of its misuse, a person who assisted her in the misuse could be liable in a secondary sense. However, consistent with the approach of equity in this area, the person would normally have to know that the recipient was abusing confidential information. Knowledge in this context would not be limited to actual knowledge, but also include "blind-eye knowledge".

13 Despite the different factual circumstances, *Vestergaard v Bestnet* offers several lessons which shed light on the correct analysis in cases of data breaches resulting from cyberattacks. The first obvious parallel is that, at a broad level, like Mrs Sig, the data controller in a cyberattack typically would not have committed any positive act of misuse or disclosure of the confidential information. This key factor distinguishes the cyberattack situation from the *Seager v Copydex* line of cases. In fact, for this reason, primary liability for breach of confidence should not attach to the data controller.

14 As for secondary liability, the Supreme Court found that Mrs Sig could not be secondarily liable for Dr Skovmand's misuse of Vestergaard's confidential information because she did not even know of such misuse. Similarly, in a cyberattack, the data controller likewise should not be held secondarily liable in breach of confidence for the cyberattacker's covert acts of data compromise or exfiltration.

III. Similar outcomes were reached in the United States and Canada

A. Approach in the United States

15 In the US, although the elements of a claim in breach of confidence vary from state to state, the claim generally appears to be predicated on an implied contract or tort, rather than equity. Yet, despite the different doctrinal basis for breach of confidence claims in the US, it is striking that recent claims by data subjects for breach of confidence against data controllers who have fallen victim to cyberattacks have not been successful.

16 *In re Capital One Consumer Data Security Breach Litigation*[14] provides a useful starting point for an analysis of the doctrinal basis for breach of confidence claims in the US. In 2019, Capital One suffered a data breach of its Amazon Web Services ("AWS") cloud environment where it stored consumers' personal information. Amazon described the attack as having occurred "due to a misconfiguration error at the application layer of a firewall installed by Capital One, exacerbated by permissions set by Capital One that were likely broader than intended. After gaining access through the misconfigured firewall and having broader permission to access resources, we believe a SSRF attack was used". The defendants, Capital One and Amazon, were aware of the AWS cloud's vulnerabilities to a SSRF attack and had jointly developed a product to address this threat by encrypting data on the AWS servers, but these efforts were allegedly inadequate. Over 100 million people in the US and six million people in Canada were allegedly affected.

17 The plaintiff credit card holders claimed that Capital One was liable for breach of confidence in taking possession of their personal information in confidence and providing inadequate data security measures to prevent its disclosure. The US District Court found that, to date, no Virginia court has recognised the tort of breach of confidence within the context of a bank–client relationship. The plaintiffs therefore failed to state a claim under Virginia law for breach of confidence.

18 However, the position was different under Florida law. This was because, in *Milohnich v First National Bank*[15] ("*Milohnich*"), a Florida Court of Appeal recognised "an implied duty on the part of a national bank not to disclose information negligently, wilfully or maliciously or intentionally to third parties, concerning the depositor's account". The US

14 488 F Supp 3d 374 (2020).
15 224 So 2d 759 (1969).

District Court thus found that the plaintiffs asserted a plausible breach of confidence claim under Florida law and dismissed the defendants' motion to dismiss in this regard.

19 It is important to conduct a deeper analysis of the jurisprudential basis for breach of confidence claims under Florida law. In *Milohnich*, the plaintiffs brought a claim against the defendant bank for negligently and intentionally divulging information concerning its accounts to third parties, resulting in the third parties suing the plaintiffs and enjoining the defendant bank from distributing their monies deposited with the bank. The majority of the District Court of Appeal of Florida found that the complaint was sufficient to state a cause of action for an alleged breach of an implied *contractual* duty. Specifically, the majority was of the opinion that the complaint "alleged a cause of action for violation of an implied duty on the part of a national bank not to disclose information negligently, wilfully or maliciously or intentionally to third parties, concerning the depositor's account".[16] It is also important to note that *Milohnich* involved a positive act of disclosure by the defendant.

20 Given that the breach of confidence claim in *Milohnich* was founded on contract, it would not be appropriate to extend its application to breach of confidence claims founded in equity. Also, crucially, the breach alleged in *Milohnich* was a positive act of disclosure. It was therefore unsurprising that the breach of confidence claim was allowed. In contrast, where data controllers are hacked by criminal cyberattackers, they typically would not have committed any positive act of disclosure or wrongful use of the data subjects' personal data. The analysis adopted in *Milohnich* therefore cannot be readily, or comfortably, extended to cyberattack cases.

21 This is borne out by more recent cyberattack cases, in which claims in breach of confidence have failed. In the case of *In Re: Ambry Genetics Data Breach Litigation*,[17] the plaintiffs' claim in breach of confidence under California law for a data breach was dismissed. The defendant genetics testing company suffered a phishing attack, resulting in a data breach in which their customers' names, dates of birth, social security numbers, medical and other personal information were allegedly exposed. The customers filed a class action against the company and its parent for, *inter alia*, breach of confidence and invasion of privacy.

16 Note, though, that Judge Pearson, in his minority judgment, took the view that the "cause of action alleged is *ex delicto*, *ie*, I think the complaint alleges that the appellee bank committed a kind of business tort". He did not think that the complaint stated a contractual cause of action, because such a complaint would have to allege facts showing the existence of an implied contract or a usage of the banking trade.

17 F Supp 3d (2021).

22 The US District Court observed that the tort for breach of confidence under California law was based upon the concept of implied obligation or contract between parties that confidential information will not be disclosed. To sufficiently allege a breach of confidence claim under California law, a plaintiff must allege that: (a) the plaintiff conveyed confidential and novel information to the defendant; (b) the defendant had knowledge that the information was being disclosed in confidence; (c) there was an understanding between the defendant and the plaintiff that the confidence be maintained; and (d) there was a disclosure or use in violation of the understanding.

23 In the absence of any allegation that the defendants had "affirmatively shared" any information or performed any act that gave information to the hackers, the court allowed the defendants' motion to dismiss the claim for breach of confidence. The court observed that California courts have found that the ordinary meaning of the word "disclosure" suggests that disclosure occurs when the healthcare provider "affirmatively shares" medical information with another person. Since the information was "involuntarily stolen" from the defendants, the claim in breach of confidence failed.

24 In *Purvis v Aveanna Healthcare LLC*,[18] the defendant paediatric home-care provider suffered a data breach through phishing techniques by a third party. Its patients, among others, brought a class action against the defendant for, *inter alia*, breach of confidence for the compromise of their personally identifiable information and protected health information. The plaintiffs argued that the defendant allowed the disclosure to happen and failed to heed warnings that its records might be targeted in a cyberattack. The US District Court dismissed the breach of confidence claim. The court explained that there was no allegation that the defendant had disclosed the plaintiffs' information; rather, the information was stolen by third parties.

25 In sum, despite the different doctrinal approach to breach of confidence claims in the US, the recent cases have still gone the way of *Warren v DSG* to find that the absence of a positive act of disclosure negatived possible claims for breach of confidence.

B. Approach in Canada

26 In *Tucci v Peoples Trust Company*,[19] the defendant was a federally-regulated trust company, which offered financial services and accounts

18 F Supp 3d (2021).
19 [2020] BCCA 246.

through its website. It maintained an unencrypted copy of a database on its webserver and failed to apply proper patches and software updates on the server. Cyberattackers allegedly from the People's Republic of China accessed its database and obtained a considerable amount of personal information about its clients. The plaintiff-clients applied to certify a class proceeding. The judge accepted that there were arguable claims for breach of contract and negligence, but not breach of confidence. He found that there was no misuse of the plaintiffs' information, as misuse required some intentional conduct by the defendant.

27 This was upheld by the British Columbia Court of Appeal, which observed:[20]

> The tort of breach of confidence is, in my view, well-defined as an *intentional* tort. The gravamen of the civil wrong is the betrayal of a confidence. Other torts, such as negligence and (assuming they exist) breach of privacy and intrusion upon seclusion are more appropriate vehicles to deal with *inadvertent* disclosure of data. [emphasis added]

28 The approach of the court here differed from that adopted in the US and English cases, in that it focused on the defendant's intention (or lack thereof) in relation to the disclosure, rather than whether the defendant had committed a positive act of disclosure. As discussed earlier, the English jurisprudence is clear that a person can be liable for breach of confidence even if he is not conscious that what he is doing amounts to misuse of confidential information.

29 Nevertheless, at their core, both approaches are founded on the same fundamental premise, namely, positive breaches are remediable through a claim in breach of confidence, but not mere carelessness. At the minimum, there must be an intentional act on the part of the defendant for liability to arise. Since the defendant here did not even commit any act, there was no need for the court to delve further into the issue of whether an unconscious, albeit positive, act can found liability.

20 *Tucci v Peoples Trust Company* [2020] BCCA 246 at [113].

IV. The approach of the English High Court to the breach of confidence claim in *Darren Lee Warren v DSG Retail Limited* should be followed in Singapore

A. Expansion of the scope for breach of confidence claims in I-Admin (Singapore) Pte Ltd v Hong Ying Ting

30 Singapore law on breach of confidence recently underwent a significant change in the case of *I-Admin*. The appellant in *I-Admin* was a Singapore-incorporated company in the business of outsourcing services and systems software, specifically, payroll administrative data processing services and human resource information systems. It operated a number of subsidiaries, including one in Shanghai. The first respondent was the appellant's former employee. As he found the appellant's software flawed, he developed a new payroll software with the second respondent, a former employee of the appellant's Shanghai subsidiary. The pair eventually incorporated a new company, the third respondent, and both resigned from their respective employers to work for the third respondent.

31 The appellant brought claims for, *inter alia*, infringement of copyright and breach of confidence against the three respondents. The appellant's claim in copyright infringement failed not least because the appellant failed to prove substantial copying. As for the claim in breach of confidence, the High Court found that the appellant's case failed on the third limb of the test in *Coco v AN Clark (Engineers) Ltd*[21] ("*Coco*") because there was no unauthorised use of its confidential information in the relevant sense. The High Court rejected the argument that the mere copying of or access to the appellant's data satisfied this requirement.

32 On appeal, the Court of Appeal ("CA") held that two distinct interests guided the operation of breach of confidence claims. The first was a plaintiff's interest in preventing wrongful gain or profit from its confidential information ("wrongful gain interest").[22] However, besides a plaintiff's wrongful gain interest, the law was also interested in protecting a plaintiff's interest to avoid wrongful loss ("wrongful loss interest"), which was suffered so long as a defendant's conscience has been impacted in the breach of the obligation of confidentiality.[23]

33 The CA held that the requirement of unauthorised use and detriment has held back the development of the law by overemphasising the wrongful gain interest at the expense of the wrongful loss interest.

21 [1969] RPC 41.
22 *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41 at [50].
23 *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41 at [53].

The CA thus set out a modified approach that should be taken in relation to breach of confidence claims. The court should first consider whether the information in question "has the necessary quality of confidence about it" and if it has been "imparted in circumstances importing an obligation of confidence".[24] Upon the satisfaction of these prerequisites, an action for breach of confidence is presumed. The burden then falls on the defendant to prove that its conscience was unaffected, for example, where the defendant came across the information by accident or was unaware of its confidential nature or believed there to be a strong public interest in disclosing it.

34 In the recent case of *Lim Oon Kuin v Rajah & Tann Singapore LLP*,[25] the CA elaborated that the modified approach in *I-Admin* only applied to cases involving alleged harm to the claimant's wrongful loss interest and, specifically, in cases involving the unauthorised acquisition of confidential information (*ie*, "taker" cases). The traditional *Coco* approach continued to apply in cases involving alleged harm to the claimant's wrongful gain interest.

35 As the facts in *I-Admin* involved harm to the appellant's wrongful loss interest, applying the modified approach, the CA in *I-Admin* found that the respondents' possession and referencing of the appellant's confidential materials constituted acts in breach of confidence, and the appellant was awarded equitable damages to be assessed.

B. The English High Court's approach to the breach of confidence claim in Darren Lee Warren v DSG Retail Limited *should be followed in Singapore*

36 The approach of the English High Court to the breach of confidence claim in *Warren v DSG* should be followed should a similar case arise in Singapore. This is notwithstanding the significant expansion of the scope for breach of confidence claims following the CA's decision in *I-Admin*. At first glance, the following *dictum* of the CA appears to impose an absolute duty on data controllers which may even extend to data security:[26]

> Depending on the circumstances under which the obligation arises, this duty may extend beyond refraining from acts of unauthorised use or disclosure. The language of 'conscience' reflects an interest in 'prevent[ing] … a wrong' … and **protecting plaintiffs from *any* kind of improper threat to the confidentiality of their information**. [emphasis added in bold; emphasis in italics in original]

24 *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41 at [61].
25 [2022] SGCA 29 at [39] and [41].
26 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [51].

37 However, the CA's comments must be understood in context. In *I-Admin*, the alleged breach lay in the acquisition, circulation and reference to the appellant's data. There was no evidence that the respondents had made unauthorised use of the appellant's data, and it was for this reason that the appellant's claim for breach of confidence failed in the High Court. Thus, the CA was really saying that even the mere copying of or access to confidential information threatens the confidentiality of information and should be actionable. Further proof of unauthorised use was not necessary to make out a successful claim in breach of confidence.

38 In *Warren v DSG*, the High Court stated that the law was clear that the action in breach of confidence imposes "a negative obligation not to disclose confidential information".[27] In so ruling, the High Court relied on, *inter alia*, the third limb of the *Coco* test, which required an unauthorised use of the confidential information. The High Court further went on to comment that framing the case as one of misuse of private information did not assist, as this latter wrong still required a positive action. The High Court gave the following illustration:[28]

> If a burglar enters my home through an open window (carelessly left open by me) and steals my son's bank statements, it makes little sense to describe this as a 'misuse of private information' by me.

39 Although this illustration was given in the context of a discussion on the English tort of misuse of private information, this analogy applies with equal force to claims in breach of confidence. Indeed, in *Warren v DSG*, the High Court struck out both the claims in breach of confidence and misuse of private information for the same reason, namely, that both were concerned with prohibiting actions by the holder of information which were inconsistent with the obligation of confidence or privacy, and it was not DSG that disclosed or misused the claimant's personal data, but the criminal third-party hackers.

40 Although the CA in *I-Admin* specifically departed from the third limb of the traditional *Coco* test in wrongful loss cases, the modified approach still requires a positive act on the part of the defendant. Copying and accessing confidential information are positive acts. The language used in other parts of the CA's decision also seemed to presume a positive

27 *Darren Lee Warren v DSG Retail Limited* [2021] EWHC 2168 (QB) at [25], citing *Sports Direct International plc v Rangers International Football Club plc* [2016] EWHC 85 (Ch) at [26].

28 *Darren Lee Warren v DSG Retail Limited* [2021] EWHC 2168 (QB) at [27].

act on the part of the defendant as a precondition of liability.[29] The CA also seemed to contemplate a positive act when it explained the shift in the burden of proof to the defendant: "plaintiffs may often be unaware of the fact that someone has done an act inconsistent with their right of confidentiality".[30]

41 In the absence of a positive act (whether of acquisition or reference to or, more conventionally, misuse or disclosure), it is difficult to argue that the defendant's conscience has been troubled so as to found a claim in breach of confidence. In *Warren v DSG*, the court cited the following passage from *Toulson & Phipps*, when explaining that a claim in breach of confidence does not encompass a data security duty:[31]

> There is a distinction between an equitable duty of confidentiality and a duty to take care to prevent confidential information or documents from falling into the hands of someone else. *The former is an obligation of conscience*, which requires the recipient not to misuse the information or documents. The latter is a duty of a different character and is not an automatic concomitant of the former. In the absence of a relevant contract, it will arise only if there is a special relationship between the parties giving rise to a duty of care under the law of negligence. [emphasis added]

42 Despite the expanded scope for liability following *I-Admin*, the modified approach still turns on the defendant's conscience having been affected. Specifically, the CA noted that in *Morison v Moat*,[32] Turner VC referred to a claim for breach of confidence as arising from an "obligation of conscience". In the CA's opinion, the use of the word "conscience" imported a broader, more fundamental, equity-based rationalisation for the protection of confidentiality. According to the CA, "[i]t places defendants under a duty; they are 'bound' not to deal with confidential information in a manner which adversely affects their conscience".[33]

43 Indeed, the equitable foundation of the cause of action in breach of confidence has a long history. In 1992, the cause of action in breach of confidence was recognised by the High Court to have equitable origins.[34] In *Wee Shuo Woon v HT SRL*,[35] the CA repeatedly used the language of

29 See *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [61], for examples given by the CA of the defendant *coming across* and *disclosing* the information.

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

31 Charles Phipps, William Harman & Simon Teasdale, *Toulson & Phipps on Confidentiality* (Sweet & Maxwell, 4th Ed, 2020) at §5-011.

32 (1851) 68 ER 492.

33 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [51].

34 *X Pte Ltd v CDE* [1992] 2 SLR(R) 575 at [23] and [26].

35 [2017] 2 SLR 94 at [31] and [32].

"conscience" or "unconscionability" to describe its equitable jurisdiction to restrain breaches of confidence. In *Adinop Co Ltd v Rovithai Ltd*,[36] the CA affirmed that, even where there was a contractual duty of confidence, there would be occasions when equity might step in to impose a duty of confidence where, for instance, the contract did not necessarily assuage conscience and equity might yet give force to conscience.

44 Although the common law does not require *conscious* misuse of the claimant's confidential information to establish a claim in breach of confidence, to take the next step of not even requiring a positive act on the part of the defendant would stretch the bounds of equity too far. In a situation where the defendant has neither committed any positive act contrary to the confidential nature of the information, nor has any intention or knowledge of having done so, it is difficult to see how his conscience is affected so as to warrant equity's intervention. As Simon Brown LJ stated in *R v Department of Health ex parte Source Informatics*,[37] "the touchstone by which to judge the scope of his duty and whether or not it has been fulfilled or breached is his own conscience, no more and no less". Although this test was criticised in *Gurry* as being too vague to be workable,[38] it has in effect been incorporated into the modified test in *I-Admin*, at the third stage. Applying the modified test in *I-Admin*, where the defendant has not committed any act contrary to the confidentiality of the data and was itself the victim of a cyberattack, the defendant should be able to discharge his burden in proving that his conscience was unaffected.

45 Solow-Niederman has advocated for tort law to develop a strict liability model for breach of confidence, so as to enable data subjects to claim where they can establish that a data breach occurred after the defendant organisation failed to meet a well-instantiated security guideline or otherwise fell below an established security standard.[39] She argued that the intervening act by the hacker should not cut off liability if the defendant's security practices and operational choices increased the probability that the intervening act could occur or made the act possible in the first instance.

46 However, it is respectfully submitted that to graft a data security duty onto a claim in breach of confidence would far exceed the equitable basis of this cause of action. Unlike its American counterpart in tort, in

36 [2019] 2 SLR 808 at [40].
37 [2001] QB 424 at [31].
38 Tanya Aplin *et al*, *Gurry on Breach of Confidence: The Protection of Confidential Information* (Oxford University Press, 2nd Ed, 2012) at para 15.09.
39 Alicia Solow-Niederman, "Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches" (2018) 127 Yale LJ Forum 614 at 631.

Singapore, the claim for breach of confidence has a recognised foundation in equity. Practically, this means that the reasonable person test suggested by Solow-Niederman cannot be comfortably imported into the breach of confidence claim in Singapore, which is ultimately founded on the defendant's conscience being adversely affected. Interestingly, as discussed above, despite their different doctrinal and analytical approaches to breach of confidence claims, the courts in the US and Canada have instinctively declined to grant relief in breach of confidence against data controllers who have suffered cyberattacks.

47 As the English High Court recognised in *Warren v DSG*, the common law action of breach of confidence creates a *negative* obligation on the part of the data controller not to act in a manner contrary to the confidentiality of the information. To impose a *positive* duty on the data controller to put in place security measures to protect the confidential information in its possession or control would stretch the law of confidence too far, and unjustifiably impinge on realms which are more properly governed by other legal regimes such as the Personal Data Protection Act 2012[40] ("PDPA"). Such other regimes can also achieve Solow-Niederman's stated objective of allocating costs to achieve optimal deterrence, by pushing data controllers to institute appropriate data security measures.

V. Conclusion

48 The law of confidence is equity's answer to situations where the defendant has dealt with information entrusted to him in a manner which adversely affects his conscience. Where the defendant has not committed any positive act with respect to the information, he can legitimately disclaim liability for breach of confidence on the ground that his conscience is unaffected.

49 While the law of confidence does not afford data subjects a remedy against data controllers who suffer cyberattacks resulting in their personal data being compromised, it does offer recourse against the cyberattacker (if legal proceedings against the cyberattacker are

40 2020 Rev Ed.

feasible).[41] As against the data controller, data subjects may have to look to another field of the law such as contract or the PDPA.

41 As the CA stated in *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [61], an obligation of confidence will also be found where confidential information has been accessed or acquired without a plaintiff's knowledge or consent.