



 DREW & NAPIER

DREWTECH SERIES

CHAPTER 12

Beset on all sides
– liability for data
breaches

19 July 2023

LEGAL UPDATE

In this Update

As cyberattacks become more prevalent, organisations have become alive to the reality of potential penalties for a data breach affecting personal data. However, this is not the end of the matter for an organization hit by a data breach. It is also possible for an organization to face civil claims from affected individuals as well as business counterparties.

This article examines what courts have said in response to the issue of civil claims arising out of data breaches, and discusses the implications that must be considered by any organization that controls data.

03
INTRODUCTION

03
EMOTIONAL DISTRESS

05
BREACH OF CONFIDENCE

06
CONCLUSION

INTRODUCTION

Imagine that your buddy Da Vinci asks you to safeguard his prized possession, the Mona Lisa, for him.

You then wake up one day to find your house broken into. Downstairs, the authorities are already standing in the doorway. "It was the Mona Lisa. She's gone", he says. "Can't you find whoever did it?" you ask. The figure of authority shakes their head. "It has already left the country. Nothing we can do about it. Oh, by the way, whoever did it didn't have a hard time because the door was unlocked, so that's a \$750,000 financial penalty". At this moment, Da Vinci comes through the door and exclaims, "You promised to safeguard the Mona Lisa for me! I want \$5 million for the distress you've caused me".

And then you actually wake up.

This may be a mere nightmare, but substitute the Mona Lisa with personal data or confidential information, and nightmare and reality start to converge.

In the wake of a data breach, stiff penalties and multiple parties coming after the company in control of the stolen data are very real possibilities, even if the perpetrators are third parties.

Under the Personal Data Protection Act 2012 (PDPA), the maximum penalty for a breach of, amongst other things, the obligation to protect personal data, is S\$1 million, or 10% of the annual turnover in Singapore of the organization for organisations whose annual turnover exceeds S\$10 million.

On top of that, the PDPA allows victims to commence a civil suit against the person(s) who caused the breach and seek compensation for their losses suffered. Caught in a cleft stick between the Personal Data Protection Commission (PDPC) and private individuals, the thoughtful handling of personal data is more imperative than ever.

EMOTIONAL DISTRESS

On 15 August 2018, one Mr. R received an unexpected email in his personal inbox. The sender addressed him by name and invited him to discuss his investment strategy as Mr. R was about to exit from a fund he had invested in. As would be expected, the fact that a stranger knew of Mr. R's personal investments came as a shock to him. It turned out that the sender was a former employee of the fund management company managing the fund in question. The former

employee had obtained Mr. R's personal data sometime during his employment.

Litigation commenced, with the fund management company as plaintiff, and the ex-employee as defendant. After some questions arose as to the standing of the fund management company to bring the lawsuit, Mr. R also joined as a plaintiff. An injunction was sought to stop the ex-employee from using certain personal data belonging to Mr. R, and an order for the ex-employee to deliver up said data. While the ex-employee eventually confirmed that he had destroyed the personal data, the lawsuit was heard by the Court of Appeal to determine an interesting question of whether Mr. R had suffered any loss or damage, which is a requirement for a civil suit under the PDPA.

The Court of Appeal ruled that "emotional distress" constituted a valid form of loss for which damages could be claimed. The following considerations were provided to determine if an individual has suffered emotional distress:

- (a) The nature of the personal data, e.g. financial data such as credit ratings are likely sensitive.
- (b) The nature of the breach, e.g. whether the breach was one-off, repeated, and/or continuing.
- (c) The nature of the defendant's conduct, e.g. whether there is fraudulent or malicious intent.
- (d) Risk of future breaches of the PDPA.
- (e) Actual impact of the breach on the claimant.

To the Court of Appeal, Mr. R was a case in point. After receiving the disturbing email from the ex-employee, Mr. R immediately emailed the fund management company and responded to the ex-employee asking him not to misuse his personal data in the future. The ex-employee failed to assure Mr. R that his personal data would be protected. In the court's eyes, Mr. R cut an anxious figure over his personal data in the hands of someone who had no right to use it.

Needless to say, the recognition of "emotional distress" as a valid form of loss could potentially expose organisations to a much wider remit of liability than if the victim had to prove monetary losses. However, this does not mean that every trivial slight will be actionable – to quote a particularly eloquent phrase from the Court: "people must learn to accept with a certain degree of stoicism the slings and arrows of this vale of tears". Negative emotions part of everyday life would not amount to emotional distress.

In this case, the fund management company was one of the plaintiffs and the defendant was an ex-employee. However, it would typically be the expectation that a claimant would pursue the employer rather than the employee, since the former would have presumably deeper pockets. Organisations would therefore be well advised (if the threat of financial penalties from the PDPC was not already sufficient incentive) to ensure that they take proper steps to handle personal data in their control.

BREACH OF CONFIDENCE

Thus far we have considered issues relating to personal data. Unfortunately, there is yet another point – confidential information which is inadvertently stolen or leaked as part of a cyberattack. It is almost inevitable today that as part of doing business, organisations will have to receive confidential information from their counterparties, whether it be secret instructions on how to manufacture a specific item or something more mundane but no less sensitive like a pricing list. Such information, if leaked, could potentially cause loss to the counterparty, who would be understandably rather cross about it, and may look to the already beleaguered victim for damages.

While there has not been a Singapore decision on this issue, the English High Court has had the opportunity to consider whether such a claim would succeed. In that case, the defendant, a retailer, was hit by a sophisticated cyberattack that resulted in the unauthorized access of personal data of customers of the defendant. One such customer commenced an action against the defendant for (amongst other things) breach of confidence.

The English Court opined that the breach of confidence claim was unsustainable, as there was no positive act that was being alleged to found the breach of confidence claim. The customer was alleging that there had been a failure on the part of the retailer to provide sufficient security for his data. However, an action for breach of confidence requires a positive action. Drawing an analogy to a situation where a burglar enters a home through an open window (carelessly left open) and steals bank statements, the Court took the view that it makes little sense to describe this as a "misuse" of information by the person leaving the window open.

This case may give some solace to an organization already fighting fires on multiple fronts, since they may be able to resist a claim for breach of confidence by a third party. However, this may be cold comfort given the organization is already mired in the difficult process of reconfiguring its systems and dealing with regularizing its own business operations. Trite as it may be, it is vastly preferable to

prevent an incident by securing the cybersecurity front, rather than dealing with the legal fallout after the fact.

Whether the position laid down by the English High Court will be followed in Singapore is yet to be determined. Another unanswered question is also whether the breached organization could be liable to other parties for different causes of action.

CONCLUSION

It is paramount for organisations in possession of data (personal, confidential, or otherwise) not to take their obligation to safeguard such data lightly (perhaps think of yourself as the guardian of the Mona Lisa?). There are multiple ways to harden the security profile of an organisation, ranging from technological methods to organizational training and policy implementation, and organisations would be well advised to consider these before it is too late.

UPDATES IN DREWTECH SERIES

1. [Chapter 1: The Importance of an Exit Strategy in Technology Contracts <6 March 2019>](#)
2. [Chapter 2: Employees, Technology and A Legal Hangover – Bring Your Own Problems? <4 June 2019>](#)
3. [Chapter 3: I host, you post, I get sued? <24 September 2019>](#)
4. [Chapter 4: Diabolus ex machina <18 February 2020>](#)
5. [Chapter 5: Bringing hygiene online – the MAS notice on cyber hygiene <28 April 2020>](#)
6. [Chapter 6: Signing without signing – contactless contracts <16 July 2020>](#)
7. [Chapter 7: My Kingdom for a Horse – When your Systems are Held to Ransom <22 January 2021>](#)
8. [Chapter 8: New risks in new skins – Updates to the Guidelines on Risk Management Practices – Technology Risk <3 March 2021>](#)
9. [Chapter 9: Of blockchains and stumbling blocks <21 July 2021>](#)
10. [Chapter 10: Service by airdrop – no parachutes required <7 July 2022>](#)
11. [Chapter 11: Large Language Models and Larger Legal Minefields <4 April 2023>](#)
12. [Chapter 12: Beset on all sides – liability for data breaches <19 July 2023>](#)

The content of this article does not constitute legal advice and should not be relied on as such. Specific advice should be sought about your specific circumstances. Copyright in this publication is owned by Drew & Napier LLC. This publication may not be reproduced or transmitted in any form or by any means, in whole or in part, without prior written approval

If you have any questions or comments on this article, please contact:



Rakesh Kirpalani

Director, Dispute Resolution &
Information Technology
Chief Technology Officer

T: +65 6531 2521

E: rakesh.kirpalani@drewnapier.com

 **DREW & NAPIER**

Drew & Napier LLC

10 Collyer Quay
#10-01 Ocean Financial Centre
Singapore 049315

www.drewnapier.com

T : +65 6535 0733

T : +65 9726 0573 (After Hours)

F : +65 6535 4906