TechTalk

Potential legal remedies when your data is exposed by your service provider

Victims could seek damages with a right of private action under PDPA and breach of contract under contract law

Ben Chester Cheong

For The Straits Times

Our personal data is strewn across so many online accounts and cloud services they are bound to leak in one way or another.

In September, coffee chain Starbucks informed customers of a data breach that compromised their rewards membership details, including name, gender, date of birth, mobile number, e-mail address and residential address. About 330,000 Singaporean Starbucks customers were reportedly affected.

In July, virtual currency exchange operator Quoine was reportedly fined $67,000 for failing to protect the personal data of more than 650,000 customers. Even though the initial breach occurred at Quoine's third-party cloud computing services provider, the Singapore Personal Data Protection Commission (PDPC) held that Quoine was responsible, as its development and operations account's security profile was not set properly and was exploited to access customer databases.

The stolen data included full names, addresses, e-mail addresses and phone numbers, including documents such as photos and scans of NRICs and passports.

PRIVATE ACTION

What are the potential legal remedies available to aggrieved individuals or victims in a data breach involving a cloud service provider? What are the limitations, if any?

The PDPC can impose financial penalties or issue directions to organisations flouting the Personal Data Protection Act (PDPA). However, these may not be satisfactory to an individual if he has personally suffered loss or damage from the data breach.

Aggrieved victims of a data breach could look at these legal remedies:

- A right of private action under the PDPA 2012; and
- A breach of contract under contract law.

In a recent case in Singapore involving the right of private action, real estate investment firms IP Investment Management and IP Real Estate Investments commenced private action against former employee Alex Bellingham, who used to manage an investment fund under the two firms.

When Mr Bellingham left to join a competitor, he contacted some of his former employers' customers, including Mr Michael Reed, who was one of the claimants. Mr Reed was concerned as Mr Bellingham has his personal data – name, personal e-mail address and investment activity in the earlier fund.

The real estate investment firms sought an injunction to restrain Mr Bellingham from using or disclosing certain personal data belonging to his former employers' customers, and an order for Mr Bellingham to deliver the said data. Damages for the distress suffered by Mr Reed and loss of control over personal data were also sought.

In a decision released in September, the Singapore Court of Appeal held that what constitutes "loss or damage" included emotional distress, thus reversing the High Court's interpretation that emotional distress is not recognised as a type of loss under the right of private action.

If an individual's personal data is compromised as a result of a data breach, often this will result in emotional distress, as personal data that is not meant to be viewed by others is released into the public domain, causing feelings of helplessness and anxiety of what their family, friends or the public might think of them.

Hence, the Singapore Court of Appeal's interpretation is a timely clarification of the scope of loss or damage under the right of private action. An individual can sue for emotional distress under the right of private action even if the individual has not suffered any financial loss.

However, this may potentially be a Pyrrhic victory for the individual, as the Court of Appeal then proceeded to clarify that a claim based on emotional distress will not succeed if it results in trivial annoyance or negative emotions that form part of the vicissitudes of life.

Similarly, Hong Kong's personal data protection legislation has made it explicit that damages may include injury to feelings.

In a decision released in February 2021, Mr Tsang Ka Kit and Ms So Siu Ki, the uncle and aunt of the claimant, Ms Tsang Po Mann, sent an anonymous letter to the primary school where Ms Tsang worked. The letter made negative allegations about Ms Tsang's character, and contained closed-circuit television images that Mr Tsang and Ms So had access to.

Ms Tsang succeeded in her claim for injury to feelings due to the misuse of personal data collected by Mr Tsang and Ms So. In Ms Tsang's witness statement, she said that she had been unable to sleep well and feared that she would be watched and filmed all the time.

As a result, she had to seek medical assistance. The Hong Kong District Court accepted Ms Tsang's argument and recognised a claimant's right to damages for injury to feelings. She was awarded compensation of HK$70,000 (S$12,700).

BREACH OF CONTRACT

In Singapore, a victim of a data breach is entitled to damages for any breach of a contract.

However, most of the cloud services contracts would have standard limitation of liability clauses that could limit their liability.

For instance, Google Cloud Platform's terms and conditions state that "neither party will have any liability arising out of or relating to the agreement for any (a) indirect, consequential, special, incidental, or punitive damages or (b) lost revenues, profits, savings, or goodwill".

In a situation where a cloud service provider declines to pay compensation on the basis of a limitation of liability clause, users could seek redress through the Unfair Contract Terms Act 1977 (UCTA). Under the UCTA, a cloud service provider cannot exclude or restrict any liability in respect of a breach by reference to any contract term, unless the contract term satisfies the requirement of "reasonableness".

In the event of a data breach, an individual could commence action against a cloud service provider and seek the court's guidance in determining whether these exclusion clauses are valid. If the exclusion clause similar to that of Google Cloud Platform's terms and conditions is recognised as valid by the courts, then it would appear that one can claim only for direct damages.

In a court case in December 2011 in the United States, payment processing firm Heartland Payment Systems disclosed that hackers had breached its computers and obtained access to payment card information of more than 100 million consumers. The firm was sued by consumers and financial institutions for breach of contract, among other claims.

The US District Court for the Southern District of Texas held that if a contract limits recovery to direct damages, a claimant may recover only the difference between the amount paid and the value received. The damages the financial institutions sought were the costs they had incurred in covering fraudulent transactions and replacing payments cards after the Heartland computer systems breach. The court held that those costs were consequential damages, but did not allow the claim since the contract breach was not wilful.

This could potentially mean that the costs of a data breach would not be covered if it covers only the subscription fee paid to the cloud service provider, which is a paltry sum, compared with the potential financial costs incurred when personal data is leaked.

An ongoing civil claim in Singapore brought by Razer against its IT solutions provider could also potentially shed more light on how the courts in Singapore would address such disputes in the future.

Razer is seeking to recover US$7 million (S$10 million) in losses from Capgemini, alleging that one of the defendant's employees was the culprit who caused a widely reported cyber-security breach in 2020 when he misconfigured and disabled the security settings of a computer server. The personal and shipping information as well as order details of about 100,000 Razer customers around the world were reportedly at risk of being exposed.

In July 2022, the IT vendor's former employee admitted in court to causing the breach that led to the customers' data leak. But it remains to be seen if the court would award the entire US$7 million in losses that Razer is seeking.

The assessment of damages would naturally be of interest to cloud service providers and users. The case could potentially set a strong precedent on how contractual disputes involving cloud service providers might develop in future.

The Personal Data Protection Commission can impose financial penalties or issue directions to organisations flouting the Personal Data Protection Act. However, these may not be satisfactory to an individual if he has personally suffered loss or damage from the data breach. PHOTO: ISTOCKPHOTO

• Ben Chester Cheong is lecturer at the Singapore University of Social Sciences' School of Law, and Of Counsel at RHTLaw Asia.