Lee Hishammuddin Allen & Gledhill

LHAG Insights

Technology, Media & Telecommunications

ABOUT THE AUTHOR

Chan Mun Yew
Partner
TMT
E: myc@lh-ag.com

23 MAY 2023

Safeguarding Secrets: Preserving Confidentiality in Information Technology (IT) & Telecommunications Projects

Information Technology (**IT**) and telecommunications projects often entail a transfer of vast amounts of sensitive, proprietary and confidential information/data between organisations. This remains the case irrespective of the magnitude and complexity of the project concerned. Breach of confidence therefore poses significant risks to organisations – it threatens the integrity of business operations and compromises the competitive advantage of businesses in the industry. It is for these reasons that the tort of breach of confidence was formulated to safeguard confidentiality in commercial transactions.

Elements of Breach of Confidence

Liability under the tort of breach of confidence arises when three elements are proven on the balance of probabilities:

(1) the information sought to be preserved must have the necessary quality of confidence;
(2) Information must have been disclosed in circumstances importing an obligation of confidence; and

(3) there must be an unauthorised use of confidential information.[1]

1st Element – Necessary Quality of Confidence

In every claim for breach of confidence, the information sought to be protected must be identified clearly and precisely. Failure to do so may result in the claim being dismissed by the Courts at the outset.[2]

Further, the law only imposes confidentiality on information that has the necessary quality of confidence. In other words, the law does not protect information which are trivial or those which are within the public domain.[3] Ultimately, the question of whether any particular information has such quality of confidence, is a question of fact to be determined by the Courts based on the factual circumstances of each individual project.

Relevant factors would include:

(a) extent of which such information is known outside of the organisation or within the industry;

(b) extent of measures taken to safeguard secrecy of such information;

(c) value of information to the organisation and its competitors;

(d) amount of effort or resources expended in developing the information; and

(e) ease or difficulty in duplicating the information.[4]

---

[1] *Seven Seas Industries Sdn Bhd v Philips Electronic Supplies (M) Sdn Bhd & Anor (Court of Appeal)* [2008] 5 MLJ 157

[2] *Dynacast (Melaka) Sdn Bhd & Ors v Vision Cast Sdn Bhd & Anor* (Federal Court) [2016] 3 MLJ 417

[3] *Worldwide Rota Dies Sdn Bhd v Ronald Ong Cheow Joon* (High Court) [2010] 8 MLJ 297

[4] *Electro Cad Australia Pty Ltd & Ors v Mejati RCS Sdn Bhd & Ors* (High Court) [1998] 3 MLJ 422

LH AG ADVOCATES AND SOLICITORS

Common examples of information with necessary quality of confidence include:- trade secrets; technology know-how or methodology; specific program codes or algorithms; technical reports; market research etc. There is no question of breach of confidence if the impugned information is within the defendant's own skill, knowledge and experience which has developed by virtue of being in the industry over the years.[5]

It is also vital to note that information will not be deemed as confidential solely by virtue of the parties' agreement alone. Irrespective of parties' agreement, the information must possess the relevant quality of confidence, in order to qualify for protection under this tort.[6]

2nd Element – Circumstances Importing Obligation of Confidence

The obligation to maintain confidentiality can be imposed expressly or impliedly. The former is quite common, as parties would often include contractual provisions in their agreements requiring the counterparty to maintain secrecy of certain information relating to the project. The latter may arise by reason of the parties' relationship. For example, where parties enter into an agreement to jointly develop a proprietary or cutting-edge technology, the law may impose an implied term in the agreement requiring both parties to maintain confidentiality of certain information relating to the project (*provided that such information possesses the quality of confidence, as examined in the 1st element above*).[7]

3rd Element – Unauthorised Use of Confidential Information

Proving unauthorised use of confidential information may not be straightforward. The law requires such unauthorised usage to be proven by way of evidence, as opposed to mere speculation or conjectures.[8]

---

[5] *Dynacast (Melaka) Sdn Bhd & Ors v Vision Cast Sdn Bhd & Anor* (Federal Court) [2016] 3 MLJ 417

[6] *Dato' Vijay Kumar Natarajan v Choy Kok Mun* (High Court) [2010] 7 MLJ 215

[7] Clerk & Lindsell on Torts (19th Edition) – paragraphs 28-11 to 28-15

[8] *Risk-X Sdn Bhd v Capital Market Risk Advisor Sdn Bhd & Ors* (High Court) [2017] 8 MLJ 475

LH AG ADVOCATES AND SOLICITORS

Unauthorised usage of confidential information can be proven via: (a) direct evidence; or (b) indirect evidence.[9]

Direct evidence would include testimony of persons who have observed the information or data being put to use, or documentary evidence showing actual usage of such information or data. Indirect evidence may be gathered from the similarities between the plaintiff's and defendant's technology in terms of design, composition, specification, behaviour (which cannot be reasonably explained without the usage of plaintiff's confidential information). Another instance of indirect evidence would be to examine the ability of the defendant to develop certain technology without the use of any impugned data or information from the plaintiff.

Remedies

If a plaintiff succeeds in proving its claim for breach of confidence, it may be entitled to the following remedies from the Court:

(i) Damages to put the plaintiff in a position as if the infringement had not occurred;

(ii) account of profits for any unauthorised usage of confidential information;

(iii) order for delivery or destruction of materials; and/or

(iv) injunction to restrain defendant from further unauthorised usage of confidential information or technology.

[9] *CMI-Centres v Phytopharm* (High Court, UK) [1999] FSR 235

Conclusion

In summary, the prospects of a successful claim for breach of confidence is highly dependent on the relevant factual circumstances. Industry players encountering issues or disputes in this area of law should therefore seek legal advice promptly to ensure that their issue/dispute can be managed effectively in their best interest.

If you have any queries, please contact Partner, **Chan Mun Yew** at (myc@lh-ag.com).

Head Office
Level 6, Menara 1 Dutamas
Solaris Dutamas
No. 1, Jalan Dutamas 1
50480 Kuala Lumpur
Malaysia
Tel: +603 6208 5888
Fax: +603 6201 0122

Johor Office
Suite 21.01
21st Floor, Public Bank Tower
No.19, Jalan Wong Ah Fook
80000 Johor Bahru, Johor
Tel: +607 278 3833
Fax: +607 278 2833

Penang Office
51-12-E, Menara BHL Bank,
Jalan Sultan Ahmad Shah,
10050, Penang
Tel: +604 299 9668
Fax: +604 299 9628

Email
enquiry@lh-ag.com

Website
www.lh-ag.com

Published by Technology, Media & Telecommunications Practice

© Lee Hishammuddin Allen & Gledhill
All rights reserved.