E-Commerce and Privacy in Singapore

By Eugene Lim & Kelry Loi,

DONALDSON & BURKINSHAW
(*Established 1874*)
Advocates & Solicitors
Notaries Public
Commissioners for Oaths
Agents for Trade Marks & Patents

24 Raffles Place #15-00 Clifford Centre
Singapore 048621
Telephone: (65) 533 9422
Telefax: (65) 533 7806, 533 3590, 5343905, 535 0809

(16 October 2001, Singapore)

General Introduction

It has been about six years since 24 October 1995, when the Council and Parliament of the European Union adopted Directive 95/46/EC (the "Data Protection Directive") on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It is natural that the existence of the European Data Protection Directive would invite the question of whether comparable laws relating to data protection exists elsewhere.

Singapore

There is, at present, no fully-developed general law of privacy in Singapore whether related to e-commerce or otherwise, to protect an individual's "right to privacy" or to prevent information relating to a person from being disseminated.

There exists, however, some distinct laws which might apply to protect confidentiality of information, depending on one's particular circumstances. For example, under section 47(1) of the Singapore Banking Act (Cap 19, 1999 Rev Edn), customer information shall not be disclosed by a bank in Singapore or any of its officers to any other person except as expressly provided in the Banking Act, and under the Singapore Legal Profession (Professional Conduct) Rules 1998 (Cap 161, S 156/98) confidential communications between a lawyer and his client are not to be disclosed without the client's consent.

Copyright

While, technically, it might be possible under the Singapore Copyright Act (Cap 63, 1999 Rev Edn) for some authors to assert copyright over documents in electronic form which they composed, it is very questionable whether this form of protection is useful as a tool for the protection of privacy. The general principle of copyright protection over original authors' works is that copyright protects the *form of expression* in the work, and not the *idea* (or information) behind the expression. Thus even if documents containing private data transmitted over the electronic medium could be protected under copyright, the form of copyright protection is very "thin" and only extends to prohibit copying of the document. It does not extend to prohibit the copying or use of the *information* in the document.

Confidence

However, very pertinent to the issue of privacy and e-commerce in Singapore is the common law relating to "breach of confidence". This is a very old cause of action, dating back for hundreds of years, which Singapore imported from English law. It has been held that where information of a confidential nature has been communicated in circumstances importing an obligation of confidentiality, an unauthorized use of the confidential information could give rise to a claim in damages, an account of profits or an injunction.

Though traditionally not really a cause of action designed for the protection of privacy in an e-commerce era, the law of confidence can be applied to some extent to protect the unauthorized dissemination of confidential information relating to oneself. We can demonstrate its potential relevance to e-commerce by studying some old English cases.

In *Seager v Copydex Ltd* [1967] 2 All ER 415, the plaintiff told the defendant about a new type of carpet grip, and the defendant commercially developed the idea which was disclosed to them in confidence. The plaintiff sued and was awarded damages to compensate him for the defendant's use of his confidential idea without having paid for it.

We could no doubt extend this general principle into the realm of e-commerce. Where a good idea for a new product has been communicated in confidence, say, by email, to a prospective investor for the latter's consideration, the law of confidence protects the communicator's confidential idea to some extent. If parties fail to reach an agreement on how to jointly exploit this new idea, and the prospective investor decides to appropriate the idea for himself and exploits it unilaterally without the communicator's authority, it could be open to the communicator to commence an action against the prospective investor for damages.

In *Prince Albert v Strange* (1849) 1 Mac & G 25, the plaintiff sued for and obtained an injunction restraining the defendant from publishing a catalogue of private etchings made by Queen Victoria and Prince Albert on subjects of private interest. The offending catalogue was compiled from copies which were made surreptitiously by a printer's

employee. Plates of the etchings had previously been sent to the printer for the purpose of making copies for the Queen and the Prince.

Thus, it is not just commercial ideas which are protected. Confidential information relating to a person's private life could also be covered under the law of confidence. Where personal data such as bank account numbers, credit card numbers, etc are disclosed to another party (say, on the Internet) for some specific and limited, commercial purpose, and under the clear understanding that the recipient of the information is to treat it as confidential, it is conceivable that the traditional law of confidence could be invoked against the unauthorized further dissemination of the information by the recipient.

There are recent signs that the English law of confidence may be evolving some novel general principles of privacy. However, it remains to be seen whether Singapore law would develop in the same direction.

Singapore Computer Misuse Act (Cap 50A, 1998 Rev Edn)

While the above relates mainly to the unauthorized dissemination of confidential information, another facet of privacy in the era of e-commerce relates to the unauthorized access to, modification and interception of, and interference with, one's computer and data / programs. For example, merchants who link up their computer systems to the Internet for commercial purposes are inevitably exposed to the threat that their systems may be the subject of unauthorized access by hackers who then introduce unauthorized alterations to their system or the data / programs contained therein.

Though this is a very invasive form of interference with data / programs stored on one's computer system, it does not *always* involve an invasion of one's "privacy". For example, the hacker's interference might extend only to material which the merchant has made freely available on the Internet, in which case, there would be nothing private about it.

In this area, the Singapore Parliament has enacted the Singapore Computer Misuse Act (Cap 50A, 1998 Rev Edn) to address such issues with the threat of criminal liability. Generally, the Singapore Computer Misuse Act ("CMA") prohibits:

(a) the unauthorized access to computer programs or data (section 3);
(b) the unauthorized modification of the contents of any computer (section 5);
(c) the unauthorized use or interception of computer services or functions (section 6);
(d) the unauthorized obstruction of interference or obstruction of the use of a computer (section 7(1)(a)); and
(e) the unauthorized impeding or preventing of access to, or impairing the usefulness / effectiveness of any computer data / programs (section 7(1)(b)).

In addition, unauthorized disclosure of passwords, access codes or other means of gaining access to any computer data / programs is prohibited under section 8 of the CMA.

Over and above the fact that the CMA prescribes severe penalties in the form of fines and / or custodial sentences, it is also provided under section 9(1) that offences committed under sections 3, 5, 6 and 7 involving certain "protected computers" will attract the enhanced punishment of a fine not exceeding S$100,000 and / or imprisonment for a term not exceeding 20 years.

The Singapore Parliament was mindful of the possible jurisdictional difficulties that computer crimes might involve. This resulted in section 11 of the CMA which extends extra-territorially, to some extent, the reach of the Act.

Further, under section 10(1), any person who abets or attempts to commit or does any act preparatory to or in furtherance of any offence under the CMA, is also guilty of that offence.

In *PP v Muhammad Nuzaihan bin Kamal Luddin* [2000] 1 SLR 34, the respondent, a 17 year old student (who hacked into servers), pleaded guilty to 3 charges of unauthorized access to computer materials, unauthorized modification of contents of a computer and unauthorized access to a computer service under sections 3(1), 5(1) and 6(1)(a) of the CMA. Fifteen other similar charges under the CMA were taken into consideration for purposes of sentencing. Yong Pung How CJ quashed the Subordinate Courts' probation order and enhanced the sentence by substituting it with an order for a total of 4 months' imprisonment. In doing so, Yong CJ quoted the Minister's speech during the Second Reading of the Computer Misuse (Amendment) Bill in Parliament:

> "In particular, during the second reading … the Minister noted … that:
>
> > '… crimes committed through the electronic medium and through use of computers are difficult to detect but they are just as serious as traditional crimes and we must equally protect our population against such crimes. To ensure that Singapore remains an attractive place for investors and businesses to operate effectively and securely, computer crimes must be treated as seriously as other criminal offences.'
>
> In the result, I had no hesitation that a deterrent sentence had to be meted out on the respondent in order to give effect to Parliament's express intention that all computer crimes will be dealt with severely in Singapore".

It is clear, therefore, that perpetrators of computer crimes in Singapore, regardless of whether they involve the invasion of personal privacy in the process, can expect no leniency from the Singapore Courts, especially if their crimes have the potential to impact deleteriously Singapore's image as a secure business place.

Conclusion

Finally, while the above sets out the general legal framework behind the protection of personal privacy in an age of e-commerce, it is also possible for parties to agree among

themselves how their rights and obligations *inter se* should be ordered. It is therefore possible for parties to expressly contract between themselves and explicitly provide for the consequences which will flow from one party's breach of the other party's confidence or privacy.

More importantly, what must be stressed in this technology-driven time is that technology may itself provide a solution to problems which the law might not yet have arrived at. It is observed, at times, that prevention may well be better than cure and that employing a self-help remedy, such as the use of firewall or encryption technology to prevent (to the extent that existing technology can) unauthorized access to confidential information, should be seriously considered. Inevitably, technological self-help remedies offer better "protection" compared to facing the uncertainties of an "after the fact" Court battle.