Current Issues in E-Commerce—Singapore

The growth of technology has made it possible for people all over the world to be connected at the touch of a button; as such, the possibilities for commercial activity has heightened tremendously with the advent of the e-Commerce movement. In Singapore, a recent survey conducted by the Infocomm Development Authority of Singapore (IDA) and Department of Statistics (DOS) revealed that e-commerce revenues had grown significantly over the past two years despite weak market sentiment. In comparison to 1999, last year saw 30% more companies with e-Commerce capabilities commencing activities. Additionally, the survey also revealed that of the 9000 companies surveyed, 98.7% frequently made use of the Internet to facilitate business applications, with online sales and purchases, online government services and software downloads being the most commonly used online applications.

1) Electronic signatures and contracting

The issues of electronic signatures and the formation of electronic contracts are thus extremely important in lieu of the increase in both B2B[1] and B2C[2] activities in Singapore. This was recognised by the Singapore government with the enactment of the Electronic Transactions Act 1998 (ETA), which is partly based on the UNCITRAL Model Law on Electronic Commerce as well as other sources[3].

The ETA aims to establish uniformity of rules regarding the authentication and integrity of electronic records as well as to promote public confidence in the integrity and reliability of electronic records and e-Commerce. In doing so, the ETA addresses the legal issues necessary to set the stage for a secure and pro-business environment for e-Commerce in Singapore.

In furtherance of these aims, the ETA lays out specific guidelines pertaining to the formation of electronic contracts and the use of digital signatures, the duties and regulation of Certification Authorities and helps facilitate the electronic applications and licenses for the public sector. The ETA also clarifies the position of network service providers' liability for third party content (addressed below under Content Liability).

Encryption and the role of Certification Authorities

Generally, "electronic signatures" are defined differently from "digital signatures" in the ETA, the latter requiring the transformation of an electronic signature through encryption techniques. To this end in a public key infrastructure network, Certification Authorities are required to engage in the role of a trusted third party to verify the identities of the signer.

Certification Authorities need not be licensed under the ETA although they are subject to the attendant duties of care, whether licensed or otherwise. The Government has opted for this voluntary licensing scheme so as to mitigate over-regulating and stifling the e-business industry. The major Certification Authority managing digital keys and certificates in Singapore is Netrust, a joint effort by the Infocomm Development Authority of Singapore and Network for Electronic Transactions (Singapore) Pte. Ltd (NETS).

2) Content liability

Intellectual Property

With regard to the protection of intellectual property rights (IPR) on the Internet, the relevant intellectual property laws apply in general. Singapore has ensured that its intellectual and copyright laws comply with the major IPR standards; for instance, the Copyright Act was amended in 1998 and 1999 to comply with our obligations under the Berne Convention and the TRIPS Accord, with the

---

[1] Business-to-Business; in this area of e-commerce, projected sales for 2001 are expected to reach S$109b, a near three-fold increase from S$40b in 1999. This healthy growth trend is seen across major sectors of the economy. (Statistics from the Infocomm Development Authority of Singapore)

[2] Business-to-Consumer; it appears that the e-lifestyle has taken root in Singapore with sales value for 2000 having increased five-fold from S$200m in 1999 to S$1.17b. Total consumer spending over the Internet is expected to reach S$2.75b by end-2001. (Statistics from the Infocomm Development Authority of Singapore)

[3] These include the State of Illinois Electronic Commerce Security Act, the Utah Digital Signature Act and German Multimedia Law.

result that works published in Singapore or created by Singapore citizens and residents are now protected by the other signatories to the Berne Convention

While there have been several keynote cases in the US and Europe on the liability of internet access service providers (IASP) in facilitating and authorising infringement of copyrighted materials, the Singapore courts have not occasioned to consider this issue. However, Part III of the ETA contains some important provisions on the liability of network service providers; in particular, subject to the conditions being satisfied, s10 of the ETA may possibly protect network service providers from liability that might arise under any "rule of law". This appears broad enough to cover copyright infringement under the Copyright Act 1987. In addition, the Copyright (Amendment) Act 1999 has now introduced a new Part IXA which sets out extensive provisions on the liability and position of network service providers.

In general, these provisions in both the Copyright Act and the ETA seek to protect a network service provider where it merely acts as a conduit for connecting users of the network with electronic copies of the material made available on the network. An example would be the making available of copyright material on the Internet on demand via a search service.

Defamation

The issue of defamation through the Internet has yet to be addressed by the Singapore courts but it is likely that defamation laws in Singapore apply in general. The law of defamation in Singapore largely follows the English common law and the following is a general definition of what amounts to defamation:

A statement is defamatory if it tends to harm the reputation of another so as to lower him or her in the estimation of the community or to deter third parties from associating or dealing with him or her.[4]

While there is no definitive authority in Singapore that electronically disseminated communications amount to libel and not slander, there is a case for the former as the electronic data posted on the database remains there until it is deleted and is therefore more than the transient form of slander as traditionally defined.

Network service providers may however, have a way out. S10 of the ETA (as mentioned above) is potentially broad enough to be used as a defence against libel suits. S10 only requires a network service provider to prove that he is firstly, a network service provider and secondly, that he merely provided access. However, the ETA lacks a technical definition of what constitutes a "network service provider" although IASPs are assumed to be within the scope of s10. This may be a potential problem in determining whether the defence covers search engine operators, for example, Yahoo and AltaVista.

3) The Computer Misuse Act

The Computer Misuse Act (CMA) first came into operation in 1993 to govern four offences:

a) unauthorized access to computer material or the hacking offence;
b) unauthorized modification of computer material;
c) unauthorized use or interception of computer services; and
d) unauthorized access with intent to commit or facilitate commission of further offences, or the ulterior-intent offence.

Subsequently, amendments were made providing for enhanced penalties for these offences and further creating two new offences:

a) unauthorized obstruction of the use of computer; and
b) unauthorized disclosure of an access code.

The objective of the CMA is to deter damage caused to computer systems. While early offences dealt mostly with hacking, as Parliament had envisioned when it enacted the Act, the computer crime spectrum has subsequently widened to include various forms of unauthorized access and the denial or interruption of computer services.

[4] This formulation is contained in the Second Restatement of Torts of the American Law Institute.

In 2000, a man was convicted for interfering with the lawful use of the Housing Development Board (HDB) mail servers by swamping the HDB with 7,500 e-mail messages within the span of 2 ½ hours. He was charged under s7 of the CMA which provides that a person who interferes interrupts or obstructs the lawful use of a computer knowingly and without any authority or lawful excuse is guilty of an offence. Another noteworthy case in 2001 saw two lawyers convicted under s3 (1) of the CMA when they were charged for unauthorized access to the database of their former employer while serving out their resignation notices. The two lawyers had on separate occasions electronically copied confidential files from their employer's computer server using a zip drive.

These two cases illustrate clearly that the expanded purview of the CMA accords well with statistical observation that computer crimes are becoming increasingly more sophisticated; in 1999, only 13 out of 185 cases of computer crime related to hacking, with figures predicted to increase in 2001. Further, the global reach of the Internet means that threats to computer networks in Singapore are not limited by geographical boundaries. It is to this end that s11 of the CMA was enacted to allow for extra-territorial jurisdiction over persons committing any of the offences recognised under the CMA, subject to the required nexus that such person or the computer, program or data be in Singapore at the material time.

Privacy and Obscenity issues

With increasing computer literacy and availability, computer crimes are taking on an added dimension of sophistication that encompasses other issues such as privacy and obscenity.

Singapore differs from the US and Europe in that we do not have a specific law governing a person's right of privacy; only information relating to governmental matters are expressly protected from unauthorised disclosure under the Official Secrets Act. Similarly, there is no common law protection of a person's right of privacy and the courts are generally reluctant to perpetuate any case law on this subject.

However, this 'right' may be protected under various laws, albeit in an attendant manner. For instance, in 1999, a man was charged under s3 (1) of the CMA with causing an e-mail server to secure unauthorised access to the electronic mailbox of an e-mail account holder. Following the termination of his relationship with the victim, the man had gained access to her electronic mailbox on 2 occasions. He went on to circulate dishonourable e-mails about the victim to her friends and colleagues as well as stalk her with the assistance of information retrieved from reading her emails. The court held that his conduct and the manner in which the offence was perpetrated warranted a deterrent sentence of 5 months imprisonment.

In general, content regulation on the Internet comes under the purview of the Singapore Broadcasting Authority (SBA). Singapore also has a light-touch class license scheme which requires IASPs and content providers to comply with an Internet Code of Practice. IASPs are also required to limit public access to 100 mass impact pornography sites. Personal communication, such as e-mail or Internet Relay Chat, personal websites and corporate Internet use by employees or for business transactions are not regulated.

On the legislative front, obscene material is specifically governed by the Undesirable Publications Act which clearly contemplates that obscene publications may be distributed via the Internet and other sources of electronic transmission. Section 6 makes it an offence to "publish, sell, offer for sale, supply, offer to supply, exhibit, distribute or reproduce any prohibited publication or extract" with the relevant punishment being a fine and imprisonment.

Conclusion

The Singapore government is cognisant of the importance of the IT Age to Singapore and besides ensuring the compliance of our legislation with international standards, has encouraged the proliferation of e-Commerce and Internet-related activities through the provision of grants and incentives and improved technical infrastructure.

Prepared by
S.Sivanesan
Marilyn Goh
Rodyk & Davidson 14 June 2001