

Paper No. 25

**REGIONAL SYMPOSIUM ON NEW MEDIA
& LEARNING TECHNOLOGIES IN ASIA**

**LEGAL CHALLENGES
IN THE
DIGITAL ENVIRONMENT**

September 8 – 10, 1999, Singapore

**Presented by Alex Thian
of
YEO WU & THIAN
Advocates & Solicitors
Agents for Trademarks & Patents**

**Tel : 323 6388
Fax : 323 6788
E-Mail : ywtlaw@singnet.com.sg**

LEGAL CHALLENGES IN THE DIGITAL ENVIRONMENT

A. THE ELECTRONIC TRANSACTIONS ACT 1998

Introduction

The Electronic Transactions Act reflects legislature's recognition of the importance of electronic commerce. Singapore is currently positioning itself to be the hub of electronic commerce as shown by our involvement in our national project known as the Electronic Commerce Hotbed Programme.

Legislature has recognised that in order for electronic commerce to flourish, transactions must be secure and obligations of parties contracting through electronic means must be legally recognised. Further, each party must be assured of the identity of the other party. Hence, there is a need to ensure that transactions can be verified and that information flow is secure. Digital certificates, digital signatures and encryption keys serve these functions.

Aims and Objectives

The aims and objectives of the Electronic Transactions Act are, inter alia, as follows:

- (i) to facilitate electronic communications by means of reliable electronic records;
- (ii) to facilitate electronic commerce;
- (iii) to eliminate barriers to electronic commerce resulting from uncertainties over writing and signature requirements;
- (iv) to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce;
- (v) to minimise the incidence of forged electronic records, intentional and unintentional alteration of records, and fraud in electronic commerce and other electronic transactions;
- (vi) to help to establish uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records;
- (vii) to promote public confidence in the integrity and reliability of electronic records and electronic commerce; and

- (viii) to foster the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium.

Signatures

(a) Electronic Signatures

The Electronic Transactions Act permits the use of electronic signatures where signatures are required as a rule of law. This means that any document which is required by law to be signed will be deemed duly signed even if an electronic signature is used.

The Electronic Transactions Act defines an "electronic signature" as any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record.

An electronic signature is deemed to be secure if, through the application of a prescribed security procedure or a commercially reasonable procedure agreed to by the parties involved, it can be verified that an electronic signature was, at the time it was made :

- (i) unique to the person using it;
- (ii) capable of identifying such a person;
- (iii) created in a manner under the sole control of the person using it; and
- (iv) linked to the electronic record to which it relates in a manner such that if the record was changed, the electronic signature would be invalidated.

Once an electronic signature is deemed secure, it shall be presumed that the secure electronic signature is the signature of the person to whom it correlates and that it was affixed by that person with the intention of signing or approving the electronic record.

(b) Digital Signatures

The Electronic Transactions Act also provides for the use of digital signatures. A digital signature is an electronic signature with added security devices through which a transacting party can be assured of the identity of the other party, the transactions can be verified and the information flow is secured.

Electronic Records

The Electronic Transactions Act gives legal recognition to electronic records. "Electronic record" is defined as a record generated, communicated, received or stored by electronic, magnetic, optical or other means in an information system or for transmission from one information system to another.

The Act expressly declares that information shall not be denied legal effect solely on the ground that it is in the form of an electronic record. The Act also provides that where a rule of law requires information to be in writing, an electronic record satisfies that requirement as long as the information contained in the electronic record is accessible so as to be usable for subsequent reference.

The Act also provides for security of electronic records. An electronic record is deemed to be secure when it is verified via a recognised security procedure.

Electronic Contracts

The legal recognition given to electronic records by the Electronic Transactions Act enables contracts to be made in electronic form. The Act provides expressly for the validity to the such contracts. This is instrumental in the promotion of electronic commerce in Singapore.

B. EVIDENCE ACT

Electronic Signatures & Record

In light of the Electronic Transactions Act, the Evidence Act has been amended to provide for the admissibility of electronic signatures and electronic records.

Previously, if a document was alleged to be signed or written by a particular person, the signature or handwriting had to be proven to be of that person's. This rule is now archaic in view of the acceptance of electronic signatures and electronic records as provided by the Electronic Transactions Act. The Evidence Act has since been amended to provide that this archaic rule shall not apply to electronic signatures or electronic records.

Evidence of Computer Output

The Evidence Act provides that computer output may be tendered as evidence in Court. However, if the Court is not satisfied that the computer output sought to be

admitted in evidence accurately reproduces the relevant contents of the original document, the Court may, in its discretion, call for further evidence.

Receiving Evidence and Documents in Court Using Information Technology

The Evidence Act provides for the possibility of filing, receiving and recording of evidence and documents in Court by the use of information technology.

There are currently two schemes devised by our Judiciary to facilitate the presentation of computer output as evidence in Court. They are as follows :

- (i) the Litigation Support System for Presentations ('LSSP'); and
- (ii) the Electronic Filing System ('EFS').

The EFS deals with the pre-trial process of filing and service of documents in Court electronically. The LSSP deals with the trial process of case presentation and presentation of evidence.

As seen above, these changes reflect the improvements to our Judiciary in line with rapid technological advancement, thereby making the Singapore Courts an attractive forum for adjudication of disputes.

C. COPYRIGHT ACT

Protection of Computer Programs

Computer programs are protected under our Copyright Act as literary works. Given the large amount of investment pumped into research and development in the IT industries, the vesting of copyright protection in computer programs is a crucial step in our copyright legislation to meet the needs of the rapid technological advancement.

Defences

The general defences such as fair use apply to computer programs. Examples of such defences include making of back-up copies and where copying or adaptations are essential to the utilisation of the computer program or possibility for software maintenance.

Recent Proposed Amendments

Proposed amendments to our Copyright Act have been introduced in Parliament on 3 August 1999. The proposed amendments aim to widen the scope of protection for materials published on the Internet and also clarify the definition of "reasonable portion".

Under the Copyright Act, a reasonable portion of a work may be copied for the purposes of research or private study. At present, "reasonable portion" is defined as not exceeding 10% of the number of pages in an edition of a work. The proposed amendments seek to extend the definition of "reasonable portion" as not exceeding 10% of the total number of bytes in an edition of a work stored in any medium by electronic means.

The proposed amendments have also sought to extend the scope of literary works to include :

- (a) a compilation in any form; and
- (b) a computer program.

"Compilation" is defined, inter alia, to include a compilation, or table, of data other than relevant materials or parts of relevant materials which, by reason of the selection and contents, constitute an intellectual creation.

As seen above, the proposed amendments reflect a step taken by legislature to address various issues arising from the use of copyright materials in a digital environment.

D. COMPUTER MISUSE ACT

Introduction

The Computer Misuse Act was enacted in light of rapid technological advancement and the inadequacy of the mainstream criminal law to address computer crimes.

Aim and Objective

The purpose of the Act is to make provision for securing computer material against unauthorised access or modification.

Offences

The Act seeks to prevent and deter computer misuse by providing that certain acts of computer misuse would constitute an offence.

Acts Constituting an Offence

Penalty

- | | | |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| 1) | Unauthorised access to computer programs and data | Fine not exceeding \$5,000 and/or imprisonment for term not exceeding 2 years |
| | | Fine not exceeding \$10,000 and/or imprisonment for term not exceeding 3 years, for 2 nd or subsequent conviction |
| | | Fine not exceeding \$50,000 and/or imprisonment for term not exceeding 7 years, if damage is caused as a result of the offence |
| 2) | Access with intent to commit or facilitate commission of offence involving property, fraud, dishonesty or causing bodily harm which is punishable on conviction with imprisonment for a term not less than 2 years | Fine not exceeding \$50,000 and/or imprisonment for term not exceeding 10 years |
| 3) | Unauthorised modification of computer material | Fine not exceeding \$10,000 and/or imprisonment for term not exceeding 3 years |
| | | Fine not exceeding \$20,000 and/or imprisonment for term not exceeding 5 years, for 2 nd or subsequent conviction |
| | | Fine not exceeding \$50,000 and/or imprisonment for term not exceeding 7 years, if damage is caused as a result of the offence |

- | | | |
|----|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| 4) | Unauthorised use or interception of computer service | Fine not exceeding \$10,000 and/or imprisonment for term not exceeding 3 years |
| | | Fine not exceeding \$20,000 and/or imprisonment for term not exceeding 5 years, for 2 nd or subsequent conviction |
| | | Fine not exceeding \$50,000 and/or imprisonment for term not exceeding 7 years, if damage is caused as a result of the offence |
| 5) | Unauthorised obstruction of use of computer | Fine not exceeding \$10,000 and/or imprisonment for term not exceeding 3 years |
| | | Fine not exceeding \$20,000 and/or imprisonment for term not exceeding 5 years, for 2 nd or subsequent conviction |
| | | Fine not exceeding \$50,000 and/or imprisonment for term not exceeding 7 years, if damage is caused as a result of the offence |
| 6) | Unauthorised disclosure of access code | Fine not exceeding \$10,000 and/or imprisonment for term not exceeding 3 years |
| | | Fine not exceeding \$20,000 and/or imprisonment for term not exceeding 5 years, for 2 nd or subsequent conviction |

Enhanced Punishment For Certain Offences

Where the offence is one which affects security, defence or international relations of Singapore, communications infrastructure, financial or public services, law

enforcement or protection of public safety, heavier penalties will be imposed.

The punishment prescribed for such offences will be a fine not exceeding \$100,000 and/ or to imprisonment for a term not exceeding 20 years.

E. THE LAYOUT-DESIGNS INTEGRATED CIRCUITS ACT 1999

Introduction

A layout-design is defined as a 3-dimensional disposition of the elements and the interconnections of an integrated circuit. An integrated circuit (hereinafter referred to as 'IC') is defined as an electronic circuit in which the elements are integrated into some medium and function as a unit.

Aims and Objectives

The Layout-Designs of Integrated Circuits Act 1999 (hereinafter referred to as 'the Act') was enacted to provide for the protection of layout-designs of integrated circuits that are created after the commencement of the Act (i.e. 15 February 1999).

The Act prevents copying and commercial exploitation of original layout-designs.

Ownership of Layout-Design

The Act provides that the owner of the layout-design shall be :

- a. the creator of the layout-design, if the layout-design is not created in pursuance of a commission or in the course of employment;
- b. the person who commissioned the layout-design, if the layout-design is created in pursuance of a commission;
- c. the employer, if the layout-design is not created in pursuance of a commission but by an employee in the course of his employment.

Duration of Protection

Under the Act, the layout-design is generally protected for a period of 15 years after the year of its creation. However, if it is first commercially exploited within 5 years after the year of its creation, it will be protected only for a period of 10 years.

Remedies for Infringement

The remedies for infringement include :

- a. damages
- b. injunctions
- c. accounts of profit
- d. order for delivery up
- e. order for disposal

However, should groundless threat of infringement be made, the person aggrieved may apply to court for:

- a. a declaration that the threat is unjustified
- b. a grant of an injunction against the continuance of the threat
- c. an award of compensation for damage sustained.

Exceptions

The Act provides for various exceptions which do not constitute infringing acts. They are as follows :

- a. copying of a part of the protected layout-design which is not original
- b. copying for a private purpose and not for commercial exploitation
- c. copying for the sole purpose of evaluation, analysis, research or teaching
- d. use of the results of such evaluation, analysis, research or teaching to create a different original layout-design
- e. copying or commercial exploitation of the layout-design referred to in (d) or any other layout-design which is independently created
- f. copying or commercial exploitation of an identical layout-design which is independently created

- g. commercial exploitation of a copy of the protected layout-design, an IC in which the layout-design is incorporated or an article that contains an IC after the copy, IC or article has already been commercially exploited
- h. innocent infringement

F. JURISDICTIONAL ISSUE

- In UK, it has been held that British Courts have jurisdiction over disputes arising from foreign Internet activities : *Meckler Media v D.C. Congress*

Under the Brussels Convention (i.e. the Brussels Convention on Jurisdiction and on the Enforcement of Judgments in Civil and Commercial Matters), an injured party is entitled to bring a claim in the place :

- a. where the tortious act was committed; or
 - b. where the resulting damage occurred.
- In U.S., it was held that even though an American Court is unable to stop Internet activity emanating from a web site abroad, it can prevent certain Internet activity from entering its jurisdiction : *Playboy v Chuckleberry*

Hence, even if an activity originated outside U.S., it may be restrained by the American Courts if it can be received in the U.S. without difficulty.