JOINT IDA-AGC REVIEW OF ELECTRONIC TRANSACTIONS ACT STAGE III: REMAINING ISSUES

(Consultation Paper)

LRRD No. 1/2005

22 June 2005

JOINT IDA-AGC REVIEW OF ELECTRONIC TRANSACTIONS ACT STAGE III: REMAINING ISSUES

CONTENTS

EXECUTIVE SUMMARY OF PUBLIC CONSULTATION ON REVIEW OF ELECTRONIC TRANSACTIONS ACT STAGE III: REMAINING ISSUES

1 The Infocomm Development Authority of Singapore and the Attorney-General's Chambers are conducting a review of the Electronic Transactions Act (ETA) and the Electronic Transactions (Certification Authority) Regulations (CA Regulations). For this purpose, a public consultation is being carried out in 3 stages dealing with electronic contracting issues, exclusions from the ETA under section 4 and other remaining issues including secure electronic signatures and certification authorities.

2 Stage I of the Public Consultation, which concerned **Electronic Contracting Issues**, was launched on 18 February 2004 and closed on 15 April 2004. Stage II of the Public Consultation, concerning **Exclusions from the ETA under section 4**, was launched on 25 June 2004 and closed on 25 September 2004. The Consultation Paper on Electronic Contracting Issues (LRRD No.1/2004) and the Consultation Paper on Exclusions from the ETA under section 4 (LRRD No.2/2004) are available on the AGC website (www.agc.gov.sg, under Publications) and the IDA website (www.ida.gov.sg, under Policy and Regulation, IDA Consultation Papers). Responses to the Consultations, available on the IDA website, are under consideration.

3 Stage III of the consultation concerns the following issues:

- Regulation of Certification Authorities
- Exemption from Liability for Internet Service Providers
- Electronic Government
- UNCITRAL Electronic Contracts Convention and Related Issues

Regulation of Certification Authorities (CAs) (Part 2)

4 IDA conducted a study comparing Singapore's CA regime under the ETA and Electronic Transactions (Certification Authorities) Regulations

with regimes in other countries. To keep the ETA up to date with developments in the CA and security solutions industry, IDA proposes to:

- Remove PKI specific references from the ETA to promote a technology neutral approach to the regulation of CAs and the authentication and security solutions market.

- Replace the voluntary licensing scheme for CAs with a voluntary accreditation scheme.

- Remove financial criteria for accreditation of CAs i.e. requirements for a banker's guarantee, insurance coverage and minimum paid-up capital.

- Reduce application fees and licensing fees for accreditation.

- Increase the duration of accreditation from 1 year to 2 years.

- Limit audit requirement to relevant security guidelines.

Exemption from Liability for Service Providers (Part 3)

5 This Part contains a survey of international developments in the exemption from liability for network service providers. The extension of section 10 of the ETA, which provides for the exemption from liability for network service providers in Singapore, to cater to the emergence of new Internet services such as content hosting services and information location tools is discussed. It is proposed that this may be done by adopting a wide definition of "network service provider" and removing the reference to "provides access" in section 10. No change is proposed to the existing exceptions in section 10(2) i.e. we do not propose to adopt any new notice and take down regime.

Electronic Government (Part 4)

6 The goal of the e-Government Action Plan II is to serve the public best with infocommunications technology by integrating services to deliver seamless and speedy service through a single point of access. Novel legal issues arise from such integration initiatives e.g. the use of combined forms, the involvement of intermediaries (including private entities) in the delivery

of Government services, the production and retention of information in electronic form and the acceptance of electronic originals.

7 Amendments are proposed to make section 47, the central provision in the ETA on Government use of electronic records, more comprehensive. Amendments are also proposed to section 9 (retention of electronic records) to provide, as a default position subject to express opt-out, that Government agencies will accept the retention of documents in electronic form. A new section 9A (on the acceptance of electronic originals) is also proposed. (A related discussion on the provision of electronic originals is also found in Part 5.) These last 2 provisions also apply generally to non-Government transactions.

UNCITRAL Electronic Contracts Convention and Related Issues (Part 5)

8 The UNCITRAL Convention on the Use of Electronic Communications in International Contracts is expected to be finalised by UNCITRAL in July 2005. We discuss the implications of various changes that have been made to the draft Convention since our previous consultation on the subject in February 2004. We seek feedback on the impact of adopting the provisions of the Convention for domestic, as well as international, contracts and for other transactions.

CONSULTATION PAPER

JOINT IDA-AGC REVIEW OF ELECTRONIC TRANSACTIONS ACT STAGE III: REMAINING ISSUES

PART I
INTRODUCTION

1.1 This Consultation Paper, which forms Stage III of a Joint IDA-AGC[1] Public Consultation on the Review of the Electronic Transactions Act, is intended to solicit the views of industry and business, professionals, the public and Government Ministries and agencies, in order to inform the Government in its review of the ETA.

1.2 This Consultation Paper on Remaining Issues concerns the following:

- Regulation of Certification Authorities
- Exemption from Liability for Internet Service Providers
- Electronic Government
- UNCITRAL Electronic Contracts Convention and Related Issues.

1.3 With the enactment of the Electronic Transactions Act (Cap.88) in 1998, Singapore became the first country in the world to enact electronic transactions legislation based on the UNCITRAL Model Law on Electronic Commerce. Since then, numerous other countries have adopted electronic commerce legislation based on the UNCITRAL model.[2]

1.4 In view of these developments overseas and internationally, the Ministry of Information, Communications and the Arts (MICA)[3], the Infocomm Development Authority of Singapore (IDA) and the

[1] Infocomm Development Authority of Singapore – Attorney-General's Chambers.
[2] See Annex D for list of recent legislation on electronic transactions and useful websites.
[3] The Ministry was previously known as MITA.

Attorney-General's Chambers (AGC) are undertaking a joint review of the Electronic Transactions Act in 3 stages. Stage I of the Public Consultation concerning Electronic Contracting Issues was launched on 18 February 2004 and closed on 15 April 2004. Stage II, relating to Exclusions from the ETA under section 4, was conducted between 25 June and 25 September 2004. Stage III forms the final Consultation Paper in this series. [4]

1.5 The ETA and related subsidiary legislation and Singapore's position with regard to the UNCITRAL Electronic Contracts Convention will be reviewed based on feedback from all 3 stages of the Joint IDA-AGC Public Consultation on the Review of the Electronic Transactions Act. Draft amendments to the ETA and related legislation will subsequently be prepared and exposed for public comment.

- Please send your feedback on this Consultation to the Law Reform and Revision Division of the Attorney-General's Chambers, marked **"Re: ETA Remaining Issues"**

  - via e-mail, at agc_lrrd@agc.gov.sg;
  - by post (a diskette containing a soft copy would be appreciated) to "**Law Reform and Revision Division, Attorney-General's Chambers, 1 Coleman Street, #05-04 The Adelphi, Singapore 179803**"; or
  - via fax, at **6332 4700.**

- Please include your personal/company particulars as well as your correspondence address, contact number and e-mail address in your response.

- The closing date for this Consultation is **17 August 2005**.

- A soft copy of the Consultation paper may be downloaded from http://www.ida.gov.sg/idaweb/pnr/index.jsp (under Consultation Papers) or http://www.agc.gov.sg (under Publications).

[4] The Consultation Paper on Electronic Contracting Issues (LRRD No.1/2004) and the Consultation Paper on Exclusions from the ETA under section 4 (LRRD No.2/2004) are available on the AGC website (www.agc.gov.sg, under Publications) and the IDA website (www.ida.gov.sg, under Policy and Regulation, IDA Consultation Papers). Responses to these Consultations, available on the IDA website, are under consideration.

- In accordance with the standard practice of IDA, responses to this Consultation (including your name and your personal/company particulars) will be posted on the IDA website. Your response may also be quoted or referred to in subsequent publications or made available to third parties. Any part of the response which is considered confidential must be clearly marked and placed as an annex to the comments raised.

- If you need any clarifications, please contact:

  - **Ms Evelyn Goh** via e-mail at evelyn_goh@ida.gov.sg; or
  - **Mrs Joyce Chao** via e-mail at agc_lrrd@agc.gov.sg.

- The Public Consultation on the Review of the ETA has been carried out in 3 stages. This Consultation on Remaining Issues forms Stage III.

PART 2
REGULATION OF CERTIFICATION AUTHORITIES

2.1 The Electronic Transactions Act ("ETA") and the Electronic Transactions (Certification Authority) Regulations ("ETR") provide a legal framework to facilitate the establishment of trusted certification authority ("CA") services in Singapore, serving both the domestic and international markets. The goal is to establish Singapore as a trusted hub for e-commerce, with its wide range of security products and services, by providing a legal foundation that is up to date with technological developments.

2.2 Having achieved the initial target of providing a basic legal framework and secure public key infrastructure ("PKI") for trusted e-commerce transactions, the focus now is to maintain the market relevance of the ETA and ETR to international developments in this area. With the emergence of a more mature PKI market and the availability of new alternative security solutions, the existing framework of the ETA and ETR, which seeks to create trust by imposing stringent requirements for licensing CAs, may be inappropriate in today's context.

2.3 This Part discusses changes to the ETA and the ETR to facilitate further development of the CA, authentication and security solutions market. IDA proposes that Singapore should move away from ensuring the business viability of CAs through stringent financial requirements. Instead, users should be allowed to make their own commercial decisions on the level of security and risk that they are prepared to accept. The revised CA framework aims to encourage CAs to be "accredited"[5] so long as the security guidelines stipulated by IDA are met.

2.4 Although the ETA is generally technology neutral, provisions relating to digital signature in Part V of the ETA are predicated on PKI technology.[6] In this Part, we discuss ways in which the ETA and ETR can be expanded to facilitate a wider coverage of all authentication technologies and solutions.

---

[5] See paragraph 2.7.

[6] PKI technology is one of the many asymmetrical algorithms used in secured e-commerce transactions and e-communication.

2.5 The following issues are discussed in this Part:

- amendments in the ETA (and ETR) to ensure technology neutrality (Part 2.6)
- change in CA licensing regime from voluntary licensing to voluntary accreditation (Part 2.7)
- removal of all financial requirements (e.g. banker's guarantee, insurance and paid-up capital) (paragraphs 2.8.1 to 2.8.11)
- reduction of the application fee for accreditation (paragraphs 2.8.12 to 2.8.16)
- increase in the term of the accreditation from 1 year to 2 years (Part 2.9)
- limitation of audit requirement to compliance with relevant security guidelines (Part 2.10)

2.6 Technology Neutral Approach

2.6.1 Like most international legislation on e-commerce[7], the ETA is generally drafted to be technology neutral. However, some of its provisions are tied to the definition of secure digital signature, which is PKI specific.

2.6.2 PKI is one of the most secure authentication architectures in terms of reliability and non-repudiation attributes. Hence, the ETA and ETR, which were intended to be the benchmark for the integrity and security of authentication services offered by CAs in e-commerce transactions, are based on the highest level of secure authentication architecture – PKI.

2.6.3 To ensure that the ETA will accord the same benefits to other new and developing technologies like biometrics, IDA proposes to remove technology specific details from the ETA[8] and leave such details to regulations to be made under the ETA.

[7] UNCITRAL Model Law on Electronic Commerce 1996 and Electronic Signatures 2001, European Commission E-Commerce Directive 2000/31/EC.

[8] In particular, from Part VI (which defines secure digital signatures and the presumptions regarding certificates and unreliable digital signature), Part VII (which describes the general duties relating to digital signatures), Part VIII (which describes the duties of Certification Authorities) and Part IX (which describes the duties of subscribers). Part V defines what constitutes secure electronic records and signatures and their related presumptions.

2.6.4 By allowing the primary legislation[9] to remain technology neutral and leaving the specific details to the regulations, the law will be able to accord new authentication technologies the same benefits as those currently enjoyed by PKI quickly and conveniently by enacting new regulations.

Q1.	Do you have any comments on the proposal to move technology specific details in the ETA[10] to the ETR?

2.7 Voluntary Licensing / Accreditation

2.7.1 Most international economies have adopted voluntary schemes[11] for the licensing or accreditation of CAs as it is more conducive to the growth of the industry. Accreditation, in particular, is used in a number of countries e.g. Australia, Japan, and Taiwan.

2.7.2 **IDA proposes to replace the current "licensing" of CAs with an "accreditation" framework.** This will better represent the voluntary nature of our CA framework. The term "licensing" is misleading as it connotes that permission must be obtained in order to operate any CA business.

Q2.	Do you have any comments on the proposal to replace the current "licensing" approach with an "accreditation" approach in the ETA and ETR? (See Annex A)

2.8 Financial Criteria and Fees

2.8.1 IDA has received industry feedback that the financial requirements to obtain a licence from the Controller of Certification Authorities ("CCA") are too stringent. In addition, the cost of an annual security audit, required under the security guidelines, is a disincentive to

[9] i.e. the ETA.
[10] i.e. Parts VI, VII, VIII and IX.
[11] The voluntary scheme provides for an opt-in scheme for CAs to be certified. Most countries that are major players in e-commerce (e.g. UK, USA, and Australia) have adopted voluntary schemes. EU's E-signature Directive prohibits its member states from imposing mandatory licensing of CAs.

applying for the CA licence (or yearly renewal), given the small CA/PKI business market in Singapore[12].

2.8.2 A study on international practices conducted by IDA[13] found that the financial requirements in the ETR are more stringent than those in other countries. Singapore's licence application fees were found to be relatively high, with an additional requirement for a banker's guarantee. These might contribute to the high barrier to entry for companies contemplating accreditation as a CA in Singapore.

2.8.3 Taking into consideration the small market size for PKI in Singapore, IDA proposes the following amendments to the existing fees and financial criteria[14].

Banker's Guarantee

2.8.4 The requirement for a $1 million banker's guarantee in the current ETR[15] was intended to increase public confidence in the adoption of the then relatively new e-commerce market, by providing a 'safety cushion' for users in the event of termination of their CA service provider.

2.8.5 However, as the technology and CA experience has matured, the requirement for a banker's guarantee is no longer necessary. First, users of CA services are usually business users who are able to make their own commercial risk assessment before engaging the services of a CA. Second, a banker's guarantee of $1 million in the small CA/PKI market in Singapore[16] is a barrier to entry.

2.8.6 IDA proposes to remove the requirement for a $1 million banker's guarantee[17].

[12] The CA/PKI business market in Singapore is presently estimated around $4 million based on a study of the Singapore PKI and Infocomm Security Market conducted by Ernst and Young in October 2004.
[13] As part of this review, IDA studied the CA Regulations and Framework of regimes from USA, UK, Australia, EU, Japan, South Korea and Hong Kong.
[14] ETR, regulations 6 and 7. See Annex A.
[15] ETR, regulation 7(1)(d). See Annex A.
[16] See footnote 12.
[17] See footnote 15.

Insurance Requirement

2.8.7 It is a good risk mitigation practice for CAs to obtain insurance coverage for errors and omissions as these are inherent CA risks[18]. However, this should be a commercial decision for each CA rather than being imposed by law. Most countries do not have such an insurance requirement.

2.8.8 IDA proposes to remove the current insurance requirement in the ETR.[19]

Paid-up Capital Requirement

2.8.9 Under the current CA licensing scheme, IDA requires applicants to prove their financial health by having sufficient paid-up capital and available financing of not less than $5 million at the time of application.

2.8.10 IDA is of the view that the capacity of a CA to set up a secured CA service data center and to have sufficient funds to continue its operations should not be scrutinised by IDA. Instead, potential clients of a CA should make their own commercial assessment of the financial health of the CA as with any other business contract.

2.8.11 IDA recommends the removal of the current paid up capital requirement in the ETR.[20]

Application Fee & Annual Licence Fee

2.8.12 Currently, CAs must pay a $5,000 application fee on every grant or renewal of a licence to be a licensed CA[21]. In addition, the CA is required to pay a $1,000 fee for each year the licence is granted. A $1,000 fee is also payable for each year the licence is renewed. In other words, a CA must pay a total of $6,000 every year that it is licensed.

[18] Including risks related to system integration, impersonation, performance delays, and delays in maintenance of the Certificate Revocation List (CRLs), key compromise, security breach and fraud.
[19] ETR, regulation 7(1)(b). See Annex A.
[20] ETR, regulation 7(1)(c). See Annex A.
[21] ETR, regulation 6(1). See Annex A.

2.8.13 The application fee of $5,000 under the existing CA licensing scheme is relatively high compared to other countries. Some countries, such as Canada and Australia, do not require any application fees from CAs.

2.8.14 IDA proposes to reduce the application fee of $5,000 to a one time fee of $1,000 to cover the administrative cost of processing the accreditation application.

2.8.15 Instead of an annual fee of $1,000 upon the grant of accreditation and subsequent renewals, with the proposal to grant accreditation and renewals for periods of 2 years at a time[22], IDA proposes that the fee for each 2 year period should remain at $1,000.

2.8.16 The total fee payable by a CA will therefore be reduced to $2,000 for the first application for a CA accreditation and $1,000 subsequently for every 2 years of renewal and accreditation.

Q3.	Do you have any comments on the proposed amendments to the financial criteria and fees for CA accreditation?

2.9 Term of Accreditation

2.9.1 CAs are currently required to conduct a security audit prior to their initial application for licensing and before each application for renewal of their licence. Since the current licence duration is 1 year, CAs are required to conduct a security audit annually.

2.9.2 Based on industry feedback that the cost of an annual security audit is a disincentive when applying for the CA licence (or its renewal), especially given the small CA/PKI business market in Singapore, **IDA proposes to increase the term of accreditation of CAs (and renewal thereof) from 1 year to 2 years.**

Q4.	Do you have any comments on the proposed increase in the accreditation duration from 1 year to 2 years?

[22] See paragraph 2.9.

2.10 Operational Criteria & Auditing Requirements

2.10.1 In order to obtain or renew their licence, CAs are required to undergo security audits to ensure that they meet the level of integrity, security and service established under the ETR and IDA security guidelines.

2.10.2 The ETR requires an applicant for a CA licence to provide an independent audit certifying its full compliance with the ETA, the ETR and the terms of its licence.

2.10.3 IDA is of the view that while the audit should check the CA's compliance with the relevant security guidelines, a comprehensive audit on the CA's compliance with the ETA, ETR and licence conditions is unnecessary. IDA proposes to remove this requirement and to limit the audit requirements to relevant security guidelines[23].

Q5.	Do you have any comments on the proposed amendments to limit the audit requirement to relevant security guidelines?[24]

[23] The removal of this requirement does not reduce IDA's ability to enforce the legislations should there be any incident of breach.

[24] i.e. removing the auditing requirement in regulation 10(1)(b) (relating to compliance with licence conditions) and (d) (relating to provisions of the ETA and ETR)

PART 3
EXEMPTION FROM LIABILITY FOR INTERNET SERVICE PROVIDERS[25]

3.1 Existing Section 10

3.1.1 The Singapore government recognises the importance of network service providers in providing information infrastructure and content and maintains that it is essential for the growth of a national information infrastructure that the exposure of network service providers to the risks of liabilities for third party content be managed. For example, an ISP should not be held liable for objectionable content or defamatory statements on the thousands of web sites that are accessed daily, and over which the ISP has no control[26]. The government also realises the impracticality in having network service providers check all content for which they merely provide access.[27]

3.1.2 Section 10 of the ETA,[28] which has been on the statute book since 1998, provides that a network service provider is not subject to criminal or civil liability for third party material for which the provider merely provides access. This section does not, however, affect the obligations of a network service provider under any licensing or other regulatory regime established under the law such as the class licensing scheme and Internet Code of Practice administered by the Media Development Authority of Singapore (MDA).[29] It also

---

[25] In this Part, the term "internet service provider" is used to refer to person providing services on the Internet such as Internet service providers (ISPs), content hosts (e.g. website hosts, bulletin board service providers, etc) and providers of information location tools (e.g. search engine operators).

[26] IDA, Salient Features of Electronic Transactions Act 1998, available at http://www.ida.gov.sg (Accessed on 3 May 2005).

[27] IDA, Electronic Transactions Act, 1 May 2002, available at http://www.ida.gov.sg (Accessed on 3 May 2005).

[28] The Explanatory Statement to the Bill stated:
"Clause 10 provides that a network service provider is not subject to criminal or civil liability for third-party material in the form of electronic records to which the provider merely provides access. The protection under this clause will not apply if the provider does something more than merely providing access to the third-party material. The clause, however, will not affect the obligations of a network service provider as such under any licensing or other regulatory regime established under any written law. The clause will also not affect any obligation founded on contract or any obligation imposed under any written law or by a court to remove, block or deny access to any material."

[29] Under the Class Licence Conditions, an ISP or relevant Internet Content Provider (ICP) has to remove or prohibit the broadcast of programmes included in its service if MDA informs the ISP or ICP that the broadcast of the programme is contrary to an applicable Code of Practice or the

does not affect any obligations founded on contract or any obligations imposed under any written law or by a court to remove, block or deny access to any material[30].

3.1.3 Section 10 of the ETA was amended by the Electronic Transactions (Amendment) Act 2004[31] to carve out liability under the Copyright Act (Cap.63) in respect of infringement of copyright or unauthorised use of any performance, the protection period of which has not expired. These amendments were made in conjunction with the Copyright (Amendment) Act 2004. The Copyright Act, as amended by the Copyright (Amendment) Act 2004 provides defences for network service providers in respect of such infringement, based on

programme is against the public interest, public order or national harmony or offends against good taste or decency.

Under the Internet Code of Practice, an ISP or relevant ICP has to use its best efforts to ensure that prohibited material is not broadcast via the Internet to users in Singapore. An ICP is to deny access to material considered by MDA to be prohibited material if directed to do so by MDA. MDA has asserted its authority to block access sparingly and has blocked 100 "mainly mass impact pornographic sites" that children could easily access. (See L.S. Malakoff, *Are You Mommy, Or My Big Brother? Comparing Internet Censorship In Singapore And the United States, 8 Pac Rim L. L Polly 423* at 443; D. Boey, "Code Of Practice For The Net Revised", Business Times, 23 October 1997, Singapore at Home & Abroad, at page 2.)

Under the Code, prohibited material is material that is objectionable on the grounds of public interest, public morality, public order, public security, national harmony, or is otherwise prohibited by applicable Singapore laws. The following factors are taken into account in considering what is prohibited material:

- whether the material depicts nudity or genitalia in a manner calculated to titillate;
- whether the material promotes sexual violence or sexual activity involving coercion or non-consent of any kind;
- whether the material depicts a person or persons clearly engaged in explicit sexual activity;
- whether the material depicts a person who is, or appears to be, under 16 years of age in sexual activity, in a sexually provocative manner or in any other offensive manner;
- whether the material advocates homosexuality or lesbianism, or depicts or promotes incest, paedophilia, bestiality and necrophilia;
- whether the material depicts detailed or relished acts of extreme violence or cruelty;
- whether the material glorifies, incites or endorses ethnic, racial or religious hatred, strife or intolerance.

A further factor that is considered is whether the material has intrinsic medical, scientific, artistic or educational value. MDA has the power to impose sanctions, including fines, on ISPs and ICPs who contravene the Code of Practice.

Information on legislation and guidelines relating to the Internet administered by MDA are available at http://www.mda.gov.sg/wms.www/devnpolicies.aspx?sid=161. The Class Licence Conditions and Internet Code of Practice may be viewed online there. (date accessed: 9 May 2005).

[30] E.g. pursuant to an injunction issued by a court on the application of an affected party.

[31] Act No. 54 of 2004

the model in the US Digital Millenium Copyright Act (DMCA)[32]. Consequently, the only defences available to a network service provider in respect of copyright and unauthorised use of performances are the defences in the Copyright Act. The Copyright (Amendment) Bill 2005[33] seeks, amongst other things, to make minor modifications to the copyright regime applicable to network service providers. Section 10 of the ETA continues to apply to network service providers in respect of all other areas, except for the exclusions in section 10(2).

3.1.4 Section 10 of the ETA, as amended with effect from 1 Jan 2005, reads:

Liability of network service providers

10.—(1) A network service provider shall not be subject to any civil or criminal liability under any rule of law in respect of third-party material in the form of electronic records to which he merely provides access if such liability is founded on —

(a) the making, publication, dissemination or distribution of such materials or any statement made in such material; or

(b) the infringement of any rights subsisting in or in relation to such material.

(2) Nothing in this section shall affect —

(a) any obligation founded on contract;

(b) the obligation of a network service provider as such under a licensing or other regulatory regime established under any written law;

(c) any obligation imposed under any written law or by a court to remove, block or deny access to any material; or

(d) any liability of a network service provider under the Copyright Act (Cap. 63) in respect of —

(i) the infringement of copyright in any work or other subject-matter in which copyright subsists; or

[32] Title 17, Chapter 5, §512, referred to as the Online Copyright Infringement Liability Limitation Act.
[33] Bill No. 12 of 2005, introduced in Parliament on 17 May 2005.

(ii) the unauthorised use of any performance, the protection period of which has not expired.

(3) For the purposes of this section —

"performance" and "protection period" have the same meanings as in Part XII of the Copyright Act;

"provides access", in relation to third-party material, means the provision of the necessary technical means by which third-party material may be accessed and includes the automatic and temporary storage of the third-party material for the purpose of providing access;

"third-party", in relation to a network service provider, means a person over whom the provider has no effective control.

3.2 New Internet Services

3.2.1 It is timely to review section 10 as the Internet has continued to evolve rapidly over the years. The variety of services and volume of content provided over the Internet has ballooned. Today new internet services are provided by means of various new technologies by a wide range of players employing different business models. Services are not limited to the provision of access to the Internet by telecommunication or broadcasting network operators[34] via their networks. It is necessary to consider whether the immunities under section 10 of the ETA should be extended to these new Internet technologies, players and activities and how the provision needs to be amended for this purpose.

3.2.2 **Content hosting services** have emerged whereby the content host may only provide storage for content on their servers and access via the Internet for such content, without providing or operating any networks of their own.[35] Commercially, content hosting usually involves the provision of computer systems with multiple web or file-transfer sites, each site with its own disk storage space and access to software facilities to add, remove and maintain the site contents. It may also provide associated system and network hardware and software to allow Internet access and specialised server software to allow Internet users to transfer copies of files stored on the system to

[34] e.g. SingTel, Starhub and M1
[35] e.g. Alta Vista.

their own computers, to view temporarily with browsers or to store on their own devices.[36] This includes personal homepages, websites, internet providers, message boards etc. Often, the content host does not play any role in creating or providing the content that it hosts. Such content may be provided by third parties without direct intervention by the content host. Hosting such content could potentially give rise to liability arising from illegal activities initiated by third parties. Liability can arise in respect of a wide variety of areas such as patents, trademarks, defamation, confidentiality, privacy, or illegal and harmful content, besides copyright.

3.2.3 The growth of services relating to Internet **information location tools** such as search engine service providers[37] is another development on the Internet. Information location tool providers carry out two main activities to help users find information on the Internet, namely, upon request by an Internet user, identifying and indexing new websites and displaying a list of links to websites where certain information is located.[38] Such service providers could face legal liability as a result of providing links to websites with infringing or illegal content insofar as they might be alleged to know the existence of the infringing or illegal material. Potential liability relating to copyright, trademark and competition violations may also arise in respect of particular linking techniques such as deep-linking[39], in-lining[40] and inclusion of certain material in links[41].[42]

3.2.4 A further new feature on the Internet comprises **aggregators**. These

[36] *"Who Is An Internet Content Host Or An Internet Service Provider (And How Is The ABA Going To Notify Them)?"* Internet Society of Australia. http://www.isoc-au.org.au/Regulation/WhoisISP.html accessed on 28 Apr 2005.
[37] e.g. Google.
[38] Esprit Project 27028 Electronic Legal Issues Platform (ECLIP) Deliverable 2.1.4 bis On-Line Intermediary Liability Issues: Comparing EU and U.S. Legal Frameworks Rosa Julia-Barcelo, accessed at europa.eu.int/ISPO/legal/en/lab/991216/liability.doc on 4 May 2005.
[39] Deep-linking consists of linking to some place other then the top level of the linked page (i.e. homepage). It may, in addition to possible copyright infringement arising from modification of copyright material, be alleged to create confusion as to the identity of the site owner or cause loss of advertising revenue by by-passing advertisements.
[40] In-lining, rather than directing the user to another website, instructs the Web browser to bring the linked image or text to the user from another website. It will automatically merge the image from the source website onto the other website. This may cause confusion as to the origin and ownership of the image.
[41] The inclusion of abstracts, famous words such as titles or trademarks, or pictures from another Website, might give rise to liability for violation of copyright or trademark laws.
[42] Esprit Project 27028, see footnote 38

are websites which provide links to a variety of sites so that, say, a user can read the headlines from multiple news sites conveniently on one page. Such aggregators link a wide variety of "upstream content" over which they may not have technical control to remove, depending on how their software code is implemented. Similarly, price comparison sites generate links to a wide variety of sites ranked by factors such as price and availability and are an important feature of the Internet in promoting consumer choice.[43]

3.2.5 Beyond these, the **P2P** (peer-to-peer) filesharing paradigm has evolved in ingenious ways since Napster. *Napster* provided filesharing services by routing user requests for a particular song or other work via a centralised index maintained by Napster. The user could then download the requested song or work directly from the location. Napster made no copies of files on its own servers. Following the Napster lawsuit, the default approach is now to employ a decentralized index. This is used by P2P services such as *Kazaa* and *Grokster*. A variation of this approach is to have a number of computers ("supernodes") act as servers hosting sub-indexes, thereby speeding up search times. *BitTorrent* demonstrates P2P services in its latest form. In this case, a particular file is not just downloaded by one user from just one other identified host or user. Instead, it is fetched from any other user who is sharing that file and the file is split into parts, each of which can be transferred independently. This improves transfer speeds enormously. *Freenet* loosely resembles *BitTorrent* in that files are downloaded and uploaded in small chunks from multiple sources, rather than as a whole, but further it encrypts files so that even a host sharing a file (or chunk thereof) cannot identify what file is being uploaded or stored.[44] These different technological configurations affect legal considerations as to knowledge and liability for unlawful content transferred via these methods.

3.2.6 The difficulties posed by the development of P2P intermediaries has been stated as follows:

[43] *Online Intermediaries and Liability for Copyright Infringement*, Charlotte Waelde and Lillian Edwards, World Intellectual Property Organization (WIPO) Seminar on Copyright and Internet Intermediaries, Geneva, 18 Apr 2005 page 24. This paper gives a comprehensive overview and analysis of international legal developments in respect of Internet intermediary liability and relevant technological developments. The seminar papers from the WIPO Seminar are available at www.wipo.int/meetings/2005/wipo_iis/en/program.html. (Accessed on 3 May 2005.)
[44] See *Online Intermediaries and Liability for Copyright Infringement*, page 7-9, see footnote 43.

> "Some form of immunity scheme for lawful P2P intermediaries may not only seem to be desirable but also essential if technological development is to continue. Yet given the essential value-neutrality of technologies, it is hard to see how a liability regime for "unlawful" and not "publicly beneficial" P2P intermediaries can be devised, except one wholly based on the intention of the service provider, such as the "active inducement" draft statutes we have seen introduced in the US. Legislation solely based on intent, however, may be difficult to prosecute and enforce."[45] [46]

3.3 Legislative Approaches to ISP Liability

3.3.1 Globally, there are 3 different approaches to service provider liability: first, the total liability approach, whereby intermediaries are treated as equally liable as content providers for unlawful content; second, the self regulation/total immunity approach; and third, the limitation of liability/notification and takedown approach. [47]

3.3.2 The first approach has not found support in the West as it "has usually been regarded as both practically unworkable, and dangerously likely to impede freedom of speech".[48]

---

[45] See *Online Intermediaries and Liability for Copyright Infringement*, page 59, see footnote 43.

[46] The **On-Line Criminal Liability Standardization Bill** introduced in the US Congress in 2002 is an example of an "active inducement" statute. The Bill seeks to amend the Federal Criminal Code to provide that no interactive computer service provider shall be liable for an offence arising from transmitting, storing, distributing or otherwise making available material provided by another person. The immunity is lost if the defendant intended that the service be used in the commission of the offence. The Bill provides that if the provider does not have such intent unless (a) an employee or agent has such intent and (b) the conduct constituting the offence was authorized, requested, commanded, performed, or tolerated by one or more members of the board of directors or a high managerial agent acting for the benefit of the provider within the scope of his office or employment. The Bill has been referred to the House Subcommittee on Crime.
"ISP Giants Support New Liability Bill" Katherine Balpataky, 18 Mar 2002, WebHost Industry Review, accessed at www.thewhir.com/features/isp031802.cfm on 27 Apr 2005, pointed out that the passage of the Bill could however take years and that further Congressional support remained to be seen.

[47] *Online Intermediaries and Liability for Copyright Infringement*, p.19–22, see footnote 43.

[48] In China, a form of strict liability is imposed on ISPs who are enjoined to refrain from "producing, posting or disseminating pernicious information that may jeopardize state security and disrupt social stability, contravene laws and regulations and spread superstition and obscenity". *Liability of Online Information Providers – Towards a Global Solution*, Chris Reed, (2003) 17(3) Int Rev LCT. Reference found in *Online Intermediaries and Liability for Copyright Infringement*, p.19, see footnote 43, which notes that access prevention provisions which would have a similar effect were dropped from the draft Australian Broadcasting Services Amendment (On Line Services) Act 1999 in the face of strong public and ISP community opposition to such an approach.

3.3.3 The second approach was based upon the expectation that service providers would for "commercial reasons, naturally take on an editorial and filtering role, so long as they are given protection from the risk of being seen as publishers, distributors or the like".

3.3.4 Section 230 of the **US Communications Decency Act**[49] is regarded as an example of the second approach. This provision has been interpreted by the courts to provide wide-ranging immunity for ISPs, however its precise scope is still being developed by the courts. It does not apply to federal criminal liability and intellectual property law.[50]

3.3.5 It has been noted, however, that this expectation of self-regulation has not altogether come to pass. "Intermediaries left to their own devices do not see content filtering as a core business activity, and will only largely remove illegal content on notice, both for fear of legal sanctions and as a matter of good public relations".[51]

3.3.6 Recent international developments in the US and Europe, namely the **US Digital Millenium Copyright Act (DMCA)**[52] and the **European E-Commerce Directive**[53] (2000/31/EC) and national laws

[49] Section 230 provides: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider".
[50] The US Court of Appeals for the Fourth Circuit held in *Zeran v America Online Inc.* 958 F.Supp. 1124 (1997) that "Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium ... Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, keep government interference in the medium to the minimum." In *Kathleen R. v City of Livermore*, the California Court of Appeals found on Mar 2001 that the immunity provisions in the CDA applied to claims for injunctive relief as wells as damage claims, even though claims for equitable relief and for waste of taxpayer funds might not readily be characterized as "tort" claims. *Legal Liability for Internet Service Providers Under the Communications Decency Act*, Edmund B. (Peter) Burke, accessed on 26 Apr 2005 at www.gigalaw.com/articles/2001-all/burke-2001-05-all.html.
[51] *Online Intermediaries and Liability for Copyright Infringement*, p.20-22, 59, see footnote 43.
[52] See footnote 32
[53] The **European E-Commerce Directive** (2000/31/EC) adopted by the European Commission deals, amongst other things, with the criminal and civil liability of e-commerce intermediary service providers. It provides for protective measures in respect of "mere conduit", caching and hosting services. These protections do not however "affect the possibility of a court or administrative authority, in accordance with Member States' legal systems, requiring the service provider to terminate or prevent an infringement" and in the case of hosting services, additionally allows, Member States to create procedures to "govern the removal or disabling of access to information" *Emerging Patterns of E-Commerce Governance in Europe – the European Union's Directive on E-Commerce* George Christou and Seamus Simpson, paper prepared for 32nd Telecommunication

implementing the Directive, have tended to take the third approach. [54] An emerging consensus can be discerned on what functions of service providers need to be protected.[55] There is however an on-going debate as to when and the extent to which service providers should be required to proactively remove, disable unlawful content.[56] Even more controversial are provisions that require service providers to proactively monitor unlawful content or to identify persons responsible for providing such content.[57]

3.3.7 Some legislation on service provider liability have taken a liability-specific (i.e. vertical) approach e.g. **UK's Defamation Act 1996**[58]

Policy Research Conference: Communication, Information and Internet Policy, George Mason University Law School, Arlington, Virginia, US, Oct 1-3, 2004. (Accessed at http://web.si.umich.edu/tprc/papers/2004/297/chris-simpTPRC04(final).pdf on 4 May 2005). This paper outlines the salient features of the legislation enacted by Finland, UK and Germany. If an activity does not qualify for exemption under the Directive, it does not mean that the service provider is automatically liable as the service provider may avail itself of other defences available under existing law.

The main areas in which they differ concern the circumstances requiring service providers to remove or disable content. The implementation deadline was 17 Jan 2002. As the liability standard set out in the Directive is a maximum standard, Member States can decide to impose less cumbersome liability criterion. *Emerging European Regime on ISP Liability* Morrison & Foerster LLP published in Computer Law Review International discusses the provisions enacted or proposed by Belgium, Finland, France, Germany, Luxembourg, Norway, Spain, Sweden. (Accessed at www.softic.or.jp/symposium/open_materials/10th/en/vinje2-en.pdf on 4 May 2005).

[54] Some other articles on such legislation: *Online Information Provider Liability for Copyright Infringement: Potential Pitfalls and Solutions*, Michael L. Siegel, 4 Va.J.L. & Tech.7, accessed on 26 Apr 2005 at www.vjolt.net/vol4/issue/v4i2a7-siegel.html; *Internet service provider liability for subscriber copyright infringement, enterprise liability, and the First Amendment*, Alfred Yen, Georgetown Law Journal accessed on 26 Apr 2005 at www.findarticles.com/p/articles/mi_qa3805/is_200006/ai_n8880509/print; *On the Service Provider Liability for Illegal Content*, Sanna Heikkinen, article in T-110.501 Seminar on Network Security 2001 ISBN 951-22-5807-2, accessed on 26 Apr 2005 at www.tml.hut.fi/Studies/T-110.501/2001/papers/index.html; *Liability Immunity for Internet Service Providers – How Is It Working?*, Heidi Pearlman Salow, Journal of Technology Law & Policy, Vol 6, Issue 1, accessed on 26 Apr 2005 at http://grove.ufi.edu/~techlaw/vol6/issue1/Pearlman.html.

[55] These relate to transitory communication or mere conduit activities, caching and hosting. Many jurisdictions also include information location services. See Part 3.5 below.

[56] See discussion at Part 3.6.

[57] See discussion at Part 3.9.

[58] UK's Defamation Act 1996 was an early precursor to legislation providing protection for service providers. Section 1 of the UK Defamation Act 1996 (so far as relevant) reads:

"(1) In defamation proceedings a person has a defence if he shows that —

(a) he was not the author, editor or publisher of the statement complained of,

(b) he took reasonable care in relation to its publication, and

(c) he did not know, and had no reason to believe, that what he did caused or contributed to the publication of a defamatory statement.

[(2) omitted.]

which relates to liability for defamation, and the US DMCA and Singapore Copyright Act which are confined to liability under those Acts. Alternatively, legislation may take a horizontal approach that applies generally in respect of all unlawful content or activities. This is the approach adopted by the EC Directive and section 10 of the Singapore ETA (except for the carve out for liability under the Copyright Act).

3.3.8 It has been questioned whether the assumptions underlying the need for service provider immunity still hold true today. A paper[59] presented at the WIPO Seminar on Copyright and Intermediaries held in Geneva on 16 April 2005 stated:

> "ISP immunity ... was based on the perception of ISPs as beleaguered defendants, facing unlimited risk as a result of hosting or providing access to limitless amounts of content over which they had little of no control. This led to a need for immunities to safeguard the public interest in a healthy Internet access market. But since then, a number of factors have altered."

3.3.9 The paper[60] proceeds to point out that "the online media industry has become more mainstreamed, and thus perhaps less in need of special protections to survive". It also asserts that "the expectation that intermediaries would naturally be driven by market forces to remove and block illegal content has not altogether come to pass. Intermediaries left to their own devices do not see content filtering as a core business activity, and will only largely remove illegal content on notice, both for fear of legal sanctions and as a matter of good

(3)A person shall not be considered the author, editor or publisher of a statement if he is only involved —
[(a) omitted.]
(c) in processing, making copies of, distributing or selling any electronic medium in or on which the statement is recorded, or in operating or providing any equipment, system or service by means of which the statement is retrieved, copied, distributed or made available in electronic form;
[(d) omitted.]
(e) as the operator of or provider of access to a communications system by means of which the statement is transmitted, or made available, by a person over whom he has no effective control.
(4) In a case not within paragraphs (a) to (e) the court may have regard to those provisions by way of analogy in deciding whether a person is to be considered the author, editor or publisher of a statement.".

[59] *Online Intermediaries and Liability for Copyright Infringement*, page 59, see footnote 43.
[60] *Online Intermediaries and Liability for Copyright Infringement*, page 59, see footnote43.

public relations; but ... even NTD[61] regimes are extremely problematic when considering the public interest and the public domain".

3.4 Issues

"Network service provider"

3.4.1 Section 10 of the ETA currently uses the term "network service provider". This term is not defined in the ETA. The reference to "network" may arguably cause the term to be interpreted to exclude those service providers that do not operate telecommunications or broadcasting networks. As noted in Part 3.2, service providers may provide services such as content hosting or information location tools without operating or providing access to networks.

3.4.2 The Copyright Act[62] contains a wide definition of the term "network service provider":

> "network service provider" —
>
> (*a*) for the purposes of section 193B[63], means a person who provides services relating to, or provides connections for, the transmission or routing of data; and
>
> (*b*) for the purposes of this Part (other than section 193B), means a person who provides, or operates facilities for, online services or network access and includes a person referred to in paragraph (*a*),
>
> but does not include such person or class of persons as the Minister may prescribe.

3.4.3 The term "service provider" is used in the US DMCA. In relation to transitory digital network communications, it is defined to mean an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material sent or received. Otherwise, it means a

[61] i.e. Notice and Takedown

[62] (Cap.63) section 193A. This section also defines "routing" (which is used in the definition) as "directing or choosing the means or routes for the transmission of data".

[63] Section 193B of the Copyright Act relates to immunity in relation to transmission, routing and provision of connections.

provider of online services or network access, or the operator of facilities therefore, including an entity described above.

3.4.4 These broad definitions appear to embrace traditional ISPs, search engines, bulletin board system operators, and even auction web sites.[64] The District Court in the *Aimster* case[65] found that Aimster, a P2P filesharing service provider,[66] did fall within the definition of an Internet service provider but held that it did not qualify under the various safe harbour provisions in the US DMCA, namely, transitory communication[67], caching[68] or information location tools[69].

3.4.5 The EC Directive applies to "information society services providers" or "intermediary service providers" which are defined by reference to the term "information society service". This is defined as "any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service".

3.4.6 The EC Directive covers not only the traditional ISP sector, but also a much wider range of actors who are involved in selling goods or services online (e.g. e-commerce sites such as Amazon and Ebay), offering online information or search tools for revenue (e.g. Google, MSN, LexisNexis or Westlaw); and "pure" telecommunications, cable and mobile communications companies offering network access services. The requirement that the service be offered "at the individual request of the recipient" however means that TV and radio broadcasters do not fall within the remit of the EC Directive, although

[64] *Online Intermediaries and Liability for Copyright Infringement*, p.11, see footnote 43.
[65] *Re Aimster* 334 F.3d 643.
[66] See description of P2P filesharing services at paragraph 3.2.5.
[67] The Aimster system worked by allowing users to communicate and transfer files via privately created networks. Thus information transferred between individual users, but did not pass through Aimster's system. *Online Intermediaries and Liability for Copyright Infringement*, p.40, see footnote 43.
[68] The Court held this provision was not applicable. *Online Intermediaries and Liability for Copyright Infringement*, p.40, see footnote 43.
[69] The Court considered that Aimster did not meet the conditions under this safe harbor because, in order to apply, a service provider cannot have actual knowledge of the infringing material or activity, or, in the absence of actual knowledge, the service provider cannot be aware of facts or circumstances from which the infringing activity is apparent. If they did have such knowledge they must take steps to remove or disable access to the material. Aimster had taken no such steps. *Online Intermediaries and Liability for Copyright Infringement*, p.40, see footnote 43.

sites which offer on-demand services such as video-on-demand are included. Certain relationships are excluded from the EC Directive as not provided wholly "at a distance". However, even if a service is provided free of charge, this does not mean that the service provider falls outside the EC Directive if the service broadly forms "an economic activity".[70]

3.4.7 The UK Electronic Commerce (EC Directive) Regulations 2002 (the UK Regulations) use the term "service provider", defined to mean a person providing an information society service. "Information society service" is defined by reference to the EC Directive.

3.4.8 As it is the intention to protect service providers in relation to content hosting or information location tools whether or not they operate or provide access to networks, the term "network service provider" should be defined in the ETA to clarify the matter. The following definition, derived from that in the Copyright Act, is proposed for discussion:

> "network service provider" means a person who provides, or operates facilities for, online services or network access and includes a person who provides services relating to, or provides connections for, the transmission or routing of data, but does not include such person or class of persons as the Minister may prescribe.[71]

3.4.9 The reference to "online services" would extend beyond traditional ISPs, search engines and bulletin board system operators, to auction web sites and even the selling of goods and services online.[72] Would such a definition extend the immunity under section 10 too widely? (See further discussion in paragraphs 3.4.15 to 3.4.22 below.)

[70] *Online Intermediaries and Liability for Copyright Infringement*, p.11, 12, see footnote 43. Recital 18 of the EC Directive clarifies. For example, it seems an employer is not an "information service provider" in terms of his employment relationship with his workers; and a doctor is not a provider of such a service so long as his advice even partially requires a "physical examination of the patient". Questions arise whether a university can avail itself of the immunity provisions if it provides personal workspace to students, if it primarily fulfils its role of providing educational services by face-to-face education rather than distance learning.

[71] We do not think that it is necessary to adopt the definition of "routing" from the Copyright Act as the term is sufficiently clear. See footnote 62.

[72] See paragraph 3.4.4.

"To which he merely provides access"

3.4.10 The words "to which he merely provides access" in section 10(1) includes caching since "provides access" is defined to mean, in relation to third-party material, the provision of the necessary technical means by which third-party material may be accessed and includes the automatic and temporary storage of the third-party material for the purpose of providing access.[73]

3.4.11 It may also arguably extend to linking whether by hyperlinking, search engine or P2P software.[74]

3.4.12 It does not however seem to extend to permanent storage or hosting (as opposed to caching).[75] Apart from traditional content hosting services, such as website hosting, bulletin boards, etc., this may also affect information location tools services which, as is common practice for search engines, cache previously retrieved material more or less permanently. This aids users in locating information in future as the material may subsequently be moved or removed from the original site.

3.4.13 One way to extend section 10 to apply to storage and hosting functions is to add express references to those functions in section 10. However, given the fast rate of evolution of Internet technology and practices, it would be hard to find language that would encapsulate all present and future functions that should be included.

3.4.14 **A simpler approach is to remove the limiting words "to which he merely provides access".** If this approach is taken and the words "to which he merely provides access" in section 10(1) are deleted, then the definition of "provides access" in section 10(3) should also be deleted as a consequential amendment. This means however that section 10 will no longer be limited to the functions mentioned in that definition i.e. providing access to material and automatic or temporary storage of material. This again raises the issue whether section 10 will

[73] Section 10(3) of the ETA.
[74] See footnote 73
[75] *Online Intermediaries and Liability for Copyright Infringement*, p.21, see footnote 43 and footnote 64 in that article. "Singapore provides total immunity to intermediary service providers but only in relation to transmission and caching liability, not, crucially, hosting."

apply too widely. (See discussion in paragraphs 3.4.15 to 3.4.22 below.)

"Third party material"

3.4.15 The reference to "third party material" in section 10(1) limits the extent of the immunity that may be claimed under section 10 to that in respect of material from "a person over whom the provider has no effective control". For example, a business selling goods or services online, cannot claim immunity under section 10 in respect of misrepresentations that it has itself made online.

3.4.16 A question arises, however, in respect of a retailer offering a product for sale online that provides a link to the manufacturer's website containing misrepresentations or misleading information concerning the product offered for sale by the retailer. Should the retailer be immune in respect of liability arising from information appearing in the manufacturer's website? Liability may conceivably arise, say, under the Consumer Protection (Fair Trading) Act[76] if a consumer reads the information via the link and is thereby misled. If section 10 applies to the retailer, he will enjoy immunity in this situation because the misleading information was third party material, presuming that the manufacturer is a person over whom the provider has no effective control. Another question may arise whether, by deliberately linking to the manufacturer's website, the retailer has adopted the information so that it ceases to be "third party material", in which case, the immunity may not apply.

3.4.17 The case of information linked by an aggregator may give rise to similar issues. An aggregator, unlike a pure search engine, may have deliberately chosen to link information from a specific website. Should a news aggregator be liable for, say, defamatory remarks appearing in newspaper articles displayed via the aggregator? Under the UK Defamation Act, such an aggregator would have to show that "he took reasonable care in relation to its publication, and he did not know, and had no reason to believe, that what he did caused or contributed to the publication of a defamatory statement". There are no such conditions in section 10 of the ETA.

[76] Cap.52A.

Regulatory schemes

3.4.18 In the US DMCA and the EC Directive, as well as the Singapore Copyright Act, the effect of the wide definitions of the terms "service providers", "information society services providers" and "network service providers" respectively is limited by the fact that the immunity granted by those legislation relates to specific functions (i.e. transitory communications, caching, hosting and additionally in the case of Singapore and US copyright legislation, information location tools)[77] and are conditional upon the obligation to remove or disable access to information in certain circumstances (i.e. upon obtaining certain knowledge or notice)[78].

3.4.19 In the case of section 10 of the ETA, the Class Licensing Scheme may serve a similar function. The obligations of a network service provider under the Class Licensing Scheme are preserved by section 10(2).[79] Under this scheme, MDA[80] has powers to issue takedown and blocking orders and internet service providers are required to comply with an Internet Code of Conduct.[81]

3.4.20 Section 10(2) of the ETA also preserves obligations "imposed under any written law or by a court to remove, block or deny access to any material".[82] A service provider would therefore have to comply with a court order or other direction made under written law requiring such removal, blocking or denial of access to material. Presumably, it is not intended that the immunity granted in section 10(1) against "civil and criminal liability" should extinguish or affect the right of the court to grant injunctive relief. In the example in paragraph 3.4.16, the court would therefore be able grant an injunction under section 9 of the Consumer Protection (Fair Trading) Act (based on the fact that there has been an unfair practice) ordering the removal of the link to the misleading content, although other remedies under that Act (such as a claim for damages) would not be available against the retailer.

[77] See further discussion of categorisation of functions in Part 3.5.
[78] See further discussion on knowledge requirements and takedown regimes in Part 3.6.
[79] Section 10(2)(b) "Nothing in this section shall affect ...(b) the obligation of a network service provider as such under a licensing or other regulatory regime established under any written law".
[80] Media Development Authority of Singapore.
[81] See footnote 29.
[82] Section 10(2)(c) "Nothing in this section shall affect ...(c) any obligation imposed under any written law or by a court to remove, block or deny access to any material".

3.4.21 Notably, the immunities under the UK Regulations[83] apply only to liability for "damages and other pecuniary remedy or for any criminal sanction". This allows injunctive relief to be sought against the service provider. Similarly, the safe harbour provisions under Singapore and US copyright laws apply only to prevent a court from granting monetary relief or making any order for infringement of copyright against the network service provider.

3.4.22 Notwithstanding the apparent width of the application of section 10 if it is amended in the manner proposed in paragraphs 3.4.8 and 3.4.14, the limitation to "third party material"[84] and the preservation of controls under the Class Licensing Scheme[85] and obligations to comply with orders to remove, block or disable access to material,[86] may provide an adequate balance.

Q6.	Is it necessary to clarify the meaning of "network service provider". Do you agree with the proposed definition of "network service provider"? (See definition proposed for discussion in paragraph 3.4.8)
Q7.	Do you agree with the proposed deletion of the words "to which he merely provides access" in section 10(1) of the ETA? (See paragraph 3.4.14)
Q8.	If section 10 of the ETA is amended as proposed in paragraphs 3.4.8 and 3.4.14, do you think any further safeguards are necessary? In particular, would the protection given under section 10 be too wide? (See paragraph 3.4.22). If yes, please elaborate with specific reference to the kinds of liability from which network service providers should not be exempted.

3.5 Alternative Approaches

Categorisation of protected functions

3.5.1 Both the EC Directive and the US DMCA define the various functions

[83] Electronic Commerce (EC Directive) Regulations 2002.
[84] See paragraphs 3.4.15 to 3.4.17.
[85] See paragraph 3.4.19.
[86] See paragraph 3.4.20.

in respect of which service providers can obtain immunity from liability. Their categorization of transmission, caching and hosting functions are markedly similar. The EC Directive does not, however, include any provision on information location tools.

3.5.2 ***Transmission, routing and provision of connections.*** This relates to the function of providing communications networks for transitory traffic. There is a consensus that service providers should not be liable for the content of traffic passing through their networks, as long as the material is handled automatically by their systems and the service provider does not store, control or modify the material.

3.5.3 The Singapore Copyright Act, based on the US DMCA, refers to "the transmission or routing by the network service provider of, or the provision of connections by the network service provider for, an electronic copy of the material through the network service provider's primary network". Immunity is subject to the conditions that (a) the transmission was initiated by or at the direction of a person other than the network service provider; (b) the transmission is carried out through an automatic technical process without any selection of the electronic copy of the material by the network service provider; (c) the network service provider does not select the recipients of the electronic copy of the material except as an automatic response to the request of another person; and (d) the network service provider does not make any substantive modification (other than any modification made as part of a technical process) to the content during the transmission through the primary network. [87] The Act also extends to transient storage by the network service provider of an electronic copy of the material in the course of such transmission, routing or provision of connections.[88]

3.5.4 The UK Regulations[89] implementing the EC Directive, have similar provisions on the "mere conduit" function. It applies to the "transmission in a communication network of information provided by a recipient of the services or the provision of access to a communication network" and includes intermediate and transient storage of information (a) which takes place for the sole purpose of

[87] (Cap.63) section 193B.
[88] (Cap.63) section 193C(1)(b).
[89] Electronic Commerce (EC Directive) Regulations 2002, regulation 17.

carrying out the transmission and (b) where the information is not stored for any period longer than is necessary for the transmission. The conditions are that the service provider (a) did not initiate the transmission, (b) did not select the transmission and (c) did not select or modify the information contained in the transmission.

3.5.5 Provisions on takedown notices do not apply to these functions since the passage of the material in question is, by definition, transitory.

3.5.6 ***Caching*** refers to the storing of Web files for later reuse so that they can be accessed more quickly by the end-user. Many service providers maintain "proxy servers" that store pages copied from the Web. When a user requests a page stored on a proxy, the service provider delivers the page quickly from the proxy rather than using the Web server to retrieve the page from the Internet.

3.5.7 The Singapore Copyright Act describes system caching as the making of a copy of material on the network service provider's primary network from another electronic copy of the material made available on a network (referred to as the originating network) through an automatic process in response to an action by a user of the primary network and in order to facilitate efficient access to the material by that user or other users.[90] The conditions for the "safe harbour" to apply are that the network service provider does not make any substantive modification (other than any modification made as part of a technical process) to the content of the cached copy of the material during the transmission of the cached copy of the material to users of the primary network or another network. In addition, the network service provider must comply with a takedown regime and any prescribed conditions relating to access to the cached copy of the material by users of the primary network or another network; the refreshing, reloading or updating of the cached copy of the material; and non-interference with technology used at the originating network to obtain information about the use of any material on the originating network, being technology that is consistent with industry standards in Singapore.

[90] (Cap.63) section 193C(1)(a).

3.5.8 The UK Regulations[91] describe caching as "automatic, intermediate and temporary storage where that storage is for the sole purpose of making more efficient onward transmission of the information to other recipients of the service upon their request". The conditions are similar to those mentioned in the preceding paragraph except that, instead of a formal takedown regime adopted by those copyright laws, service provider must act "expeditiously to remove or to disable access to the information he has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.[92]

3.5.9 ***Storage of third party material.*** This is one aspect of content hosting.[93] (See description of content hosting activities in paragraph 3.2.2).

3.5.10 The Singapore Copyright Act[94] protects "storage, at the direction of a user of the network service provider's primary network, of an electronic copy of the material on the primary network. The conditions to be satisfied are that the service provider does not receive any financial benefit directly attributable to the copyright infringement if the provider has the right and ability to control the infringing activity. The service provider must remove or disable access to the material if it acquires actual knowledge of the infringement or knowledge of facts or circumstances which would lead inevitably to

[91] Electronic Commerce (EC Directive) Regulations 2002, regulation 18
[92] Electronic Commerce (EC Directive) Regulations 2002, regulation 17.
" ... the service provider -
(i) does not modify the information;
(ii) complies with conditions on access to the information;
(iii) complies with any rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
(iv) does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
(v) acts expeditiously to remove or to disable access to the information he has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement."
[93] See description of content hosting in paragraph 3.2.2 above.
[94] (Cap.63) section 193D(1)(a).

the conclusion that the copyright in the material has been infringed,[95] or pursuant to provisions for takedown notices. There are also provisions to restore material pursuant to counter notices.

3.5.11 The UK Regulations[96] provide immunity in respect of "storage of information provided by a recipient of the service" who "was not acting under the authority or the control of the service provider" if it "does not have actual knowledge of unlawful activity or information and, where a claim for damages is made, is not aware of facts or circumstances from which it would have been apparent to the service provider that the activity or information was unlawful" or "upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information".

3.5.12 ***Information location tools.*** This refers to the referral or linkage to an online location where third party material is accessible e.g. via a search engine. (See description of information location tools in paragraphs 3.2.3 to 3.2.5 above).

3.5.13 The Singapore Copyright Act[97], modeled on the US DMCA, protects "the network service provider referring or linking a user of any network to an online location on a network (referred to ... as the originating network), being a location at which an electronic copy of the material is made available, by the use of an information location tool such as a hyperlink or directory, or an information location service such as a search engine". The conditions for immunity are the same as those for content hosting. (See paragraph 3.5.10 above.) The legislative history of the DMCA explicitly recognises that constructive knowledge should not be imputed to a human compiled directory provider "simply because the provider viewed an infringing site during the course of assembling the directory" and only if information location tool providers turn a blind eye to "red flags" of obvious infringements will they not qualify for safe harbour.[98]

[95] The Copyright (Amendment) Bill (Bill No. 12 of 2005), introduced on 17 May 2005, amends section 193D(3) to widen the court's discretion to determine whether a network service provider should be treated as having the requisite knowledge.
[96] Electronic Commerce (EC Directive) Regulations 2002, regulation 19.
[97] (Cap.63) section 193D(1)(b).
[98] Esprit Project 27028, page 22, see footnote 38.

3.5.14 The European Directive however contains no provision on information location tools and instead placed this issue under a "re-examination procedure", i.e. the European Commission allows itself a period of 3 years following adoption of the EC Directive to re-evaluate the importance of addressing the scope of liability of information location tool providers and hyperlink providers. According to the Esprit report, the reason given is that Member States laws' (and courts) are unlikely to render information location tool providers liable for mere provision of links to infringing sites, as the lack of case law on this topic demonstrates. The Esprit report however points out that a review of copyright statutes, general liability rules, and recent case law may lead to a different conclusion.[99]

3.5.15 A number of European Member States have already included immunity for information location tools under their national laws.[100]

3.6 Obligation to Remove or Disable Material

3.6.1 As noted above, the immunities for the provision of caching,[101] hosting[102] and information location tool services[103] are conditional upon compliance with the obligation to remove or disable material in certain circumstances. These circumstances may relate to the service provider's knowledge of certain matters or receipt of notice in a specific form.

3.6.2 ***Obligation to takedown upon knowledge.***[104] Knowledge requirements vary according to the function being performed by the service provider. In the case of caching, the UK Regulations[105] require the service provider to remove content if it has actual knowledge that offending content has been removed at the original source, or access to it there has been disabled, or that such removal or disablement has been ordered by a court or administrative authority. In contrast, in

[99] Esprit Project 27028, page 22, see footnote 38.
[100] eg. Spain's 2001 draft Bill, Article 17, deals with linking in a manner similar to the DMCA. *Emerging European Regime on ISP Liability* Morrison & Foerster LLP, see footnote 53.
[101] See paragraphs 3.5.6 to 3.5.8.
[102] See paragraph 3.5.10.
[103] See paragraph 3.5.13.
[104] The German working draft of 1 Dec 2000 adopted the "actual knowledge" or with regard to claims for damages "awareness of facts or circumstances" (constructive knowledge). *Emerging European Regime on ISP Liability* Morrison & Foerster LLP, see footnote 53.
[105] Electronic Commerce (EC Directive) Regulations 2002, regulation 17.

relation to hosting,[106] a service provider must remove content if it acquires actual knowledge of the unlawful activity or content and is aware of facts or circumstances from which the illegality of the activity or content should have been apparent. The obligation to remove, in this case, arises from actual knowledge as well as knowledge that the service provider ought to have known based on the facts or circumstances actually known to it (i.e. constructive knowledge). The UK Regulations have not prescribed procedures for takedown notices, relying instead on codes of conduct and the creation of voluntary measures, with the Department of Trade and Industry retaining an oversight role.

3.6.3 The scheme under the Singapore Copyright Act is modeled on the US DMCA regime. In the case of hosting and referral services, it imposes an obligation to takedown material upon actual or constructive knowledge (similar to the UK Regulations[107] in respect of hosting services) or upon prescribed notice under a takedown regime. In the case of caching, however, the service provider is not required to remove content unless it has received notice in the prescribed form[108] in the takedown regime.

3.6.4 One criticism of imposing a duty on service providers to remove or disable material upon acquiring knowledge is the "chilling effect" it has upon freedom of expression. Service providers "are likely to takedown material upon receipt of almost any type of notice, even if later that notice proves to have been unfounded, and they are likely to include provisions in their user's agreements permitting them to remove material at their discretion. Freedom of expression will thereby be controlled by host service providers and bulletin board operators who would understandably prefer to shut a site down or eliminate certain content than expose themselves to liability".[109]

3.6.5 The requirement to act "expeditiously" has also been criticised for being too vague. It is pointed out that service providers might need to take legal or other advice to determine whether they have "actual knowledge" of illegal activities or materials in some instances, e.g. in

[106] Electronic Commerce (EC Directive) Regulations 2002, regulation 19.
[107] Electronic Commerce (EC Directive) Regulations 2002.
[108] The Copyright (Amendment) Bill (Bill No. 12 of 2005) seeks to clarify that the notice may be "substantially in accordance with" the prescribed form.
[109] Esprit Project 27028, see footnote 38.

relation to defamation or confidentiality, difficult issues of law may arise which can only be determined with certainty by a court of law. In such cases, it may not be appropriate to expect a service provider to evaluate the validity of complaints in order to decide whether to comply with a notice to takedown certain material.[110]

3.6.6 In an attempt to address such criticism, the UK Regulations[111] provide guidance in determining when a service provider has actual knowledge via a non-exhaustive list of criteria. Although the UK Regulations do not adopt a prescribed notice and takedown regime, whether a service provider has received a notice in accordance with contact details provided by the service provider and the details given in such a notice are circumstances that are to be taken into account to determine if the service provider has actual knowledge.[112]

3.6.7 **Notice and takedown regime.** An alternative to the "knowledge approach" is to adopt a regime whereby service providers have no obligation to remove material unless and until they receive formal notice in a prescribed form requiring them to do so. This approach takes the guesswork out of determining whether and when service providers must takedown material.

[110] Norway consulted on 2 proposals. The first proposal limits liability for hosting services if the service provider expeditiously removes or blocks access to content if it (a) is made aware that the court or a public authority has prohibited the making of content (b) has been notified in accordance with the notice and takedown regime or (c) has actual knowledge that the content is illegal "under intellectual property, child pornography, or racism law". The proposal states there may be areas in respect of which it is inappropriate to apply a knowledge test as it involves difficult legal evaluations e.g. defamation, hence the proposed limitation to specified areas of law. The second alternative excludes the knowledge test. *Emerging European Regime on ISP Liability* Morrison & Foerster LLP, see footnote 53.

[111] Electronic Commerce (EC Directive) Regulations 2002.

[112] Electronic Commerce (EC Directive) Regulations 2002, regulation 22.

"**Notice for the purposes of actual knowledge**

22. In determining whether a service provider has actual knowledge for the purposes of regulations 18(b)(v) and 19(a)(i), a court shall take into account all matters which appear to it in the particular circumstances to be relevant and, among other things, shall have regard to -

(a) whether a service provider has received a notice through a means of contact made available in accordance with regulation 6(1)(c), and

(b) the extent to which any notice includes –

(i) the full name and address of the sender of the notice;

(ii) details of the location of the information in question; and

(iii) details of the unlawful nature of the activity or information in question."

3.6.8 There are various ways of implementing such an approach. Under the Singapore Copyright Act[113], service providers can be certain that they are protected by the "safe harbour" provisions so long as they comply with prescribed procedures under the takedown regime. The notices must be purportedly made by the owner of the copyright in the material or under his authority, state certain prescribed matters, and be given to the service provider's designated representative.[114]

3.6.9 This method is, however, still hotly debated internationally. One concern is it that service providers will not be adequately proactive in taking down unlawful material even though they may have actual knowledge of it. It may be considered appropriate in certain contexts, for public policy reasons, to impose obligations on service providers to exercise greater vigilance, e.g., in respect of certain types of material such as illegal pornographic material (especially child pornography) or hate speech.[115] It was suggested that Sweden did not implement the notice and takedown regime probably because of explicit concern that such a regime would limit the ways in which an intermediary can become aware of illegal material and take it down, and that a notice and take-down regime might be difficult to combine with their existing laws on criminal liability of electronic bulletin boards which imposes criminal liability on operators of electronic bulletin boards who intentionally or grossly negligently fail to takedown certain material.[116]

3.6.10 An opposing criticism is that service providers will be too quick to takedown material upon receipt of a notice as they will have no regard whether the notice is reasonably justified.

3.6.11 The takedown regime under the Singapore Copyright Act[117] attempts to balance these issues by requiring the service provider to expeditiously take reasonable steps to notify the person who made

[113] Modeled on the US DMCA.
[114] Norway and Sweden also adopt notice and takedown regimes modeled on the US DMCA provisions. *Emerging European Regime on ISP Liability* Morrison & Foerster LLP, see footnote 53.
[115] Finland's draft proposal in 2001 required service providers to remove material on their own initiative upon obtaining knowledge in relation to certain criminal matters e.g. child pornography. *On the Service Provider Liability for Illegal Content* Sanna Heikkinen accessed at www.tml.hut.fi/Studies/T-110.501/papers/index.html on 27 Apr 2005. Also *Emerging European Regime on ISP Liability* Morrison & Foerster LLP, see footnote 53.
[116] *Emerging European Regime on ISP Liability* Morrison & Foerster LLP, see footnote 53.
[117] Modeled on the US DMCA provisions.

available the material and restore such material to the network (subject to technical and practical feasibility) if that person submits a counter notice in the prescribed form,[118] unless the owner of the copyright in the material has, before the restoration, commenced proceedings to prevent such restoration.

3.6.12 Another way of addressing the concern that takedown notices can be, and have been, made without proper justification is to have a centralised authority to evaluate and convey demands for material to be taken down to service providers.

3.6.13 In the area of child pornography, a non-governmental "quango", the Internet Watch Foundation[119], has existed in the UK since 1996 to provide a means by which the ISP industry as a whole can receive notice and directions as to whether allegedly illegal content complained about by the public should be taken down. This enables takedown requests to be scrutinised rather than possibly simply complied with by individual service providers lacking time and legal resources. It is also to some extent transparent, as statistics are issued about the types of complaints and action taken. On the other hand, the Rightswatch project funded by the EC from 2002-2003 failed to gain support because of a lack of consensus between the interests of the various stakeholders in the market. This has been suggested to be a "strong indication of the obstacles to agreement among stakeholders on voluntary NTD[120] regimes, absent statutory underpinnings".[121]

3.6.14 Other models somewhere between NTD[122] and a full court hearing are possible. In Belgium, takedown of content by an ISP must be authorized not by a full court but by a state prosecutor. In Italy and Spain, EC Directive-based regulations demand that "a competent body" determine the legality of disputed content. In the UK, the Publisher's Association, have proposed a scheme whereby as soon as "takedown" is opposed by the provider of the disputed content, the

[118] The Copyright (Amendment) Bill (Bill No. 12 of 2005) seeks to clarify that the notice may be "substantially in accordance with" the prescribed form.

[119] See http://www.iwf.org.uk, accessed on 17 May 2005. It has recently also begun to scrutinize racist and hate speech material.

[120] i.e. Notice to Takedown.

[121] *Online Intermediaries and Liability for Copyright Infringement*, p.32 – 34, see footnote 43.

[122] See footnote 120.

matter must mandatorily go to the courts and the content meanwhile remain in the public view.[123]

3.6.15 The Oxford PCMLP-IAPCODE[124] research identifies a number of essential requirements for a self regulatory dispute resolution system to work effectively and in the public interest in the digital media/content area. The Study recommends that such schemes should amongst other things, be beneficial to consumers; accessible to members of the public; independent from interference by interested parties; adequately funded and staffed; provide effective and credible sanctions; provide for auditing and review by the relevant independent regulatory authority; be publicly accountable; and provide for an independent appeals mechanism.[125] The Oxford research suggests[126] that the way forward may lie with codes of conduct developed by relevant industry bodies accredited by the relevant independent regulatory authority for that industry sector. [127]

3.6.16 **Takedown only in compliance with order of court or regulatory authority.** Another way is to leave the administration of such demands to a judicial or regulatory authority. In this case, the service provider only has to act in compliance with orders of the court or relevant authority. This approach provides certainty for the service provider and assurance that demands to takedown material are justified.

3.6.17 One possible consequence of limiting compliance to orders from a court or regulatory authority is that service providers would have no incentive to be proactive. The problems with placing obligations upon service providers to remove material proactively have, however, been pointed out above.

---

[123] *Online Intermediaries and Liability for Copyright Infringement*, p.32 – 34, see footnote 43. Article refers to oral presentation by Publishers Association representative, Not-Con, London, June 5, 2004.

[124] Oxford PCMLP-IAPCODE "Self regulation of digital media converging onto the Internet: Industry codes of conduct in sectoral analysis" available at http://pcmlp.socleg.ox.ac.uk/execsummary.pdf, accessed on 19 May 2005.

[125] Oxford PMCLP-IAPCODE, para 12.1, see footnote 124.

[126] Oxford PMCLP-IAPCODE, section 12: Watching the Watchdogs: Accreditation of Self-regulatory Codes and Institutions, see footnote 124.

[127] Referenced from *Online Intermediaries and Liability for Copyright Infringement*, p.32 – 34, see footnote 43.

3.6.18 Another consequence is that private parties will have to incur legal costs in seeking a court order against the service provider before such material will be removed. It seems justifiable that the service provider should not bear the cost of obtaining a court order since section 10 is intended to protect service providers from civil liability and the obligation to takedown arguably arises only when the service provider is aware of the court order. The party seeking removal of the material may, in any case, be able to recover the costs incurred from the party liable for providing the material. It remains to be seen how a Singapore court might decide such an issue. The considerations of the UK Court of Appeal in the case outlined in the next paragraph may be equally relevant to the situation where a service provider requires a court order before complying with a request to takedown third party material.

3.6.19 In an unreported decision (December 19, 2001) , which arose from proceedings in *Totalise v Motley Fool* [2001] EMLR 29, the UK Court of Appeal held that the party (a service provider) asked to disclose the identity of a user of its services should *not* have to meet the costs of the court order for disclosure if that party had a genuine doubt that the applicant was entitled to disclosure, and that they might be legally obliged not to disclose and could be subject to legal proceedings if they disclosed voluntarily (as was possible there since the disclosure breached the terms of the privacy policy).[128]

3.6.20 A regime requiring takedown only upon a court order or an order by a regulatory authority seems to work well. In the case of material that has to be taken down for reasons of public policy, it is appropriate that a responsible regulatory authority should be empowered to issue such orders as an executive authority is well-placed to decide issues of public policy. In the case of an assertion of private rights, it seems justifiable that the private party should initiate court proceedings to obtain a court order for the takedown of third party material and that the service provider should not have to bear the costs of obtaining the court where there is uncertainty as to the validity the private claim.

3.6.21 **The existing regime under section 10 of the ETA in effect follows this model.** The amendments discussed in paragraphs 3.4.1 to 3.4.14 above provide service providers with blanket immunity with respect to

[128] *Online Intermediaries and Liability for Copyright Infringement*, page 52, see footnote 43.

civil and criminal liability in respect of third party material. This immunity is, amongst others[129], subject to the obligations of a network service provider as such under a licensing or other regulatory regime established under any written law[130] e.g. the Class Licensing scheme, and any obligation imposed under any written law or by a court to remove, block or deny access to any material[131].

3.7 Protection for Removing or Disabling Content

3.7.1 The Singapore Copyright Act[132] provides that a service provider shall not be liable to any person in respect of any action taken by it in good faith in relation to the removal or disabling of access to, or removal of, material in reliance on a notice or knowledge referred to under that Act. This is subject to the requirement to notify the person who made available the material and other requirements relating to restoration of the material upon receipt of a counter notice. This protection applies whether or not it is ultimately determined that there was an infringement of copyright. Similar protection is provided in respect of restoration of material in accordance with a counter notice. Other jurisdictions with a notice to takedown regime also provide protection for service providers complying with the takedown regime.[133]

3.7.2 It has been suggested that Finnish law does not contain such a provision because under Finnish contract and tort law, it would be difficult to imagine a case where the service provider would be liable for complying with the law.[134]

3.7.3 Such a provision does not seem to be necessary in the case of section 10 of the ETA since compliance with obligations under the Class Licensing Scheme or a court order would not give rise to liability on the part of service providers.

[129] The other exceptions are obligations founded on contract and obligations under the Copyright Act: section 10(2)(a) and (d) respectively.
[130] ETA, section 10(2)(b)
[131] ETA, section 10(2)(c)
[132] Section 193DA, modeled on the US DMCA
[133] Under the Australian Act, Internet content hosts and ISPs have immunity from civil proceedings in respect of compliance with access-prevention notices and take-down notices respectively issued by the regulator. Broadcasting Services Act, 5th Schedule, s.84(2) and (3).
[134] *Emerging European Regime on ISP Liability* Morrison & Foerster LLP, see footnote 53.

3.8 Burden of Proof in Criminal Proceedings

3.8.1 The UK Regulations[135] provide that, where a service provider, charged with an offence in criminal proceedings arising from transmission, provision of access or storage of material relies on the defences in the regulations[136], the service provider only needs to adduce evidence sufficient to raise an issue with respect to that defence. The prosecution will then have to prove beyond reasonable doubt that the defence applies.

3.8.2 The Singapore Copyright Act similarly contains a provision requiring the court to presume, in the absence of evidence to the contrary, that the network service provider has complied with various conditions under the Act if the service provider adduces evidence to that effect.

3.8.3 Such provisions make it easier for a service provider to rely on the relevant defences by lessening the burden of proof on the service provider. **Such provision is however probably unnecessary in respect of defences claimed under section 10 of ETA since that provision is uncomplicated. It does not contain any of the additional conditions imposed by laws modeled upon the US DMCA[137] or EC Directive[138].**

3.9 Other Obligations

3.9.1 Various European countries have laws to aid the identification of anonymous or pseudonymous users who provide unlawful content. For example, French law requires service providers to keep records of the actual identity of customers to allow their identification.[139] Spanish law allows a court to request a service provider to monitor a specified recipient of the service and keep information regarding that person's activities, for a maximum of 6 months.[140] Luxembourg's law foresees the possibility for courts to require the monitoring of specific

[135] Electronic Commerce (EC Directive) Regulations 2002.
[136] i.e. regulations 17,18, or 19. See discussion above in paragraphs 3.5.4, 3.5.8 and 3.5.11.
[137] Singapore Copyright Act, see paragraphs 3.5.3, 3.5.7 and 3.5.9.
[138] E.g. the UK Regulations see paragraphs 3.5.4, 3.5.8 and 3.5.11.
[139] The French Freedom of Communications Act of 1986 as amended on 22 Aug 2000. *Emerging European Regime on ISP Liability* Morrison & Foerster LLP, see footnote 53.
[140] Spanish draft Bill 2001 Article 11. *Emerging European Regime on ISP Liability* Morrison & Foerster LLP, see footnote 53.

sites or general surveillance for periods of time when necessary for public order, the prevention and investigation of crime, public health and public safety or the safety of consumers[141]

3.9.2 Spanish law also imposes a duty to inform authorities upon gaining knowledge of existence of illegal activity.[142] Sweden has a law imposing criminal liability on operators of electronic bulletin boards who intentionally or grossly negligently fail to takedown certain material.[143]

3.9.3 The Singapore Copyright (Amendment) Bill 2005[144] seeks to amend the Copyright Act to clarify that the "safe harbour" provisions are not conditional on a service provider "monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with any standard technical measure" or "gaining access to, removing or disabling access to any electronic copy of any material in any case where such conduct is prohibited by law".[145]

3.10 Summary

3.10.1 The issues in considering an appropriate takedown regime may be summarized as follows:

> "It might usefully be asked what is desired – *post* publication removal or blocking of Internet content only on the demand of a properly empowered institution or court, thus respecting all legal defenses and the public interest; or some degree of cheap speedy restraint on illicit Internet content by the operation of NTD.[146] If we want the latter, can we introduce an element of public scrutiny more effective than the put-back rules of the DMCA? The issue here is really what body (if any) should adjudicate on notice and takedown - judicial or administrative, self-regulatory or with a more public constitutionalised role, industry funded or state funded, open or acting behind closed doors." [147]

[141] *Emerging European Regime on ISP Liability* Morrison & Foerster LLP, see footnote 53.
[142] Spanish draft Bill 2001 Article 11. *Emerging European Regime on ISP Liability* Morrison & Foerster LLP, see footnote 53.
[143] *Emerging European Regime on ISP Liability* Morrison & Foerster LLP, see footnote 53.
[144] Bill No. 12 of 2005, introduced in Parliament on 16 May 2005.
[145] Proposed amendment to section 193A(3) of the Copyright Act.
[146] i.e. Notice to Takedown.
[147] *Online Intermediaries and Liability for Copyright Infringement*, footnote 43, page 32, see footnote 43.

3.10.2 The regime under section 10 of the ETA governs the civil and criminal liability of service providers in respect of third party materials, apart from liability under the Copyright Act and contractual obligations. [148] It seeks to provide service providers with certainty as to their liability. The obligation to remove or disable third party material may arise under a licensing or other regulatory regime established under any written law[149] e.g. the Class Licensing scheme, and obligations imposed under any written law or by a court to remove, block or deny access to any material[150].

3.10.3 **This regime requires takedown only upon a court order or order by an appropriate regulatory authority.** It has worked well. In the case of material that has to be taken down for reasons of public policy, the power to order material to be removed or disabled is vested in a regulatory authority[151]. In the case of an assertion of private rights, the matter is adjudicated by a court and the service provider is only required to act pursuant to a court order.

3.10.4 **Since section 10 does not impose conditions on service providers in order to benefit from immunity in respect of different functions, there is no need to categorise functions as in the Copyright Act and the EC Directive.** A self regulatory takedown regime would necessitate such categorisation since a network service provider's responsibility to takedown material would depend on what function it is performing.

Q9.	Should the immunity regime for service providers under section 10 of the ETA be changed (other than the changes mentioned in Q.6, 7 and 8)?

[148] Section 10(2)(d) and (a) respectively.
[149] ETA, section 10(2)(b)
[150] ETA, section 10(2)(c)
[151] Media Development Authority of Singapore in respect of the Class Licensing Scheme and Internet Code of Conduct.

PART 4
ELECTRONIC GOVERNMENT

4.1 The Government's electronic government initiative, e-Government Action Plan II (eGAP II), sets its core intent as delighting customers and connecting citizens. The goal is to serve the public best with infocommunications technology, in particular, by integrating services to deliver seamless and speedy service through single points of access.

4.2 Having achieved the target of providing practically all Government services online in eGAP I, the focus in eGap II is on integrating the delivery of such services through initiatives such as the Online Business Licensing Service, Integrated Trade and Logistics IT platform, National Electronic Payment Hub and Moving House Online. The new service delivery paradigm is 3P (public-private-people) Integration.[152]

4.3 The new paradigm, not surprisingly, gives rise to new legal ramifications. The integrated delivery of services means that the customer (by what seems to him to be a single transaction) is in fact carrying out multiple transactions. Such multiple transactions may involve dealings with one or more Government (or private) agencies governed under the same or different pieces of legislation.

4.4 This Part discusses changes to the ETA to facilitate further developments in e-Government. Although the existing law already contains various provisions relating to e-Government, in some respects it may not go far enough to harness the full potential of new technology to provide fully integrated services through single points of access. The proposed amendments to the ETA to facilitate e-Government are set out in **Annex B**.

4.5 The following issues are discussed in this Part:

- the use of electronic means in transactions with the Government, in particular electronic forms for the integrated delivery of Government services (Parts 4.7 and 4.8);

[152] Keynote Address by Acting Minister for Finance, Mr Raymond Lim at the e-Government Forum 2004 (28 October 2004), accessed at www.egov.gov.sg/e-Government+Forum+2004.htm.

- the involvement of intermediaries in the integrated delivery of Government services (Part 4.9);

- the retention of documents in electronic form (Part 4.10);

- the acceptance of electronic originals (Part 4.11); and

- other issues relating to the production of information in electronic form (Part 4.12).

The issues referred to in Parts 4.10 to 4.12 are not limited to government transactions, but encompass private transactions, as well. They are discussed here for convenience as they are, to a large extent, particularly relevant to government transactions.

4.6 Existing Law

4.6.1 The Legal Infrastructure for E-Government was harmonised and expanded in 1998 by the ETA which arose out of the recommendations of the Electronic Commerce Hotbed Study Group on Legal, Regulatory and Enforcement Issues[153]. The provisions of the **ETA** are generally applicable to Government transactions. Below, we highlight two provisions of the ETA which have particular relevance to e-Government.

4.6.2 **Section 47 of the ETA[154]** is the central provision that enables Government agencies[155] to adopt electronic means of carrying out

[153] The full text of the Study Group's report can be found at www.lawnet.com.sg (under Legal Workbench, Publications).

[154] Section 47 is set out below for ease of reference:

Acceptance of electronic filing and issue of documents

47. —(1) Any department or ministry of the Government, organ of State or statutory corporation that, pursuant to any written law —

(a) accepts the filing of documents, or requires that documents be created or retained;

(b) issues any permit, licence or approval; or

(c) provides for the method and manner of payment,

may, notwithstanding anything to the contrary in such written law —

(i) accept the filing of such documents, or the creation or retention of such documents in the form of electronic records;

(ii) issue such permit, licence or approval in the form of electronic records; or

(iii) make such payment in electronic form.

government functions without the need to enact additional laws. It allows Government agencies to accept the filing, creation or retention of documents in the form of electronic records.

4.6.3 **Section 9 of the ETA[156]**, which allows electronic records to satisfy legal requirements for the retention of records, applies to

(2) In any case where a department or ministry of the Government, organ of State or statutory corporation decides to perform any of the functions in subsection (1) (i), (ii) or (iii), such agency may specify —

(a) the manner and format in which such electronic records shall be filed, created, retained or issued;

(b) where such electronic records have to be signed, the type of electronic signature required (including, if applicable, a requirement that the sender use a digital signature or other secure electronic signature);

(c) the manner and format in which such signature shall be affixed to the electronic record, and the identity of or criteria that shall be met by any certification authority used by the person filing the document;

(d) control processes and procedures as appropriate to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(e) any other required attributes for electronic records or payments that are currently specified for corresponding paper documents.

(3) Nothing in this Act shall by itself compel any department or ministry of the Government, organ of State or statutory corporation to accept or issue any document in the form of electronic records.

[155] By Government agencies, we mean to refer to any department or ministry of the Government, organ of state or statutory board.

[156] Section 9 is set out below for ease of reference:

Retention of electronic records

9. —(1) Where a rule of law requires that certain documents, records or information be retained, that requirement is satisfied by retaining them in the form of electronic records if the following conditions are satisfied:

(a) the information contained therein remains accessible so as to be usable for subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) such information, if any, as enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received, is retained; and

(d) the consent of the department or ministry of the Government, organ of State or the statutory corporation which has supervision over the requirement for the retention of such records has been obtained.

(2) An obligation to retain documents, records or information in accordance with subsection (1) (*c*) shall not extend to any information necessarily and automatically generated solely for the purpose of enabling a record to be sent or received.

(3) A person may satisfy the requirement referred to in subsection (1) by using the services of any other person, if the conditions in paragraphs (*a*) to (*d*) of that subsection are complied with.

(4) Nothing in this section shall —

(a) apply to any rule of law which expressly provides for the retention of documents, records or information in the form of electronic records; or

(b) preclude any department or ministry of the Government, organ of State or a statutory corporation from specifying additional requirements for the retention of electronic records

requirements for retention which are under the supervision of Government agencies, but only with the consent of such Government agency.

4.6.4 In addition, the **Interpretation Act**[157] has various provisions that facilitate the use of electronic means. First, it provides that authority to make subsidiary legislation includes the authority to provide for the manner and method in which any document, record, application, permit, approval or licence may be submitted, issued or served by electronic means, or for the authentication thereof.[158]

4.6.5 Second, the Interpretation Act also provides that authority to provide for fees and charges includes the authority to provide for the determination of the manner and method of payment. This includes payment by electronic means.[159]

---

that are subject to the jurisdiction of such department or ministry of the Government, organ of State or statutory corporation.

[157] Sections 2 (definition of "prescribed"), 7 and 20 are set out for ease of reference:

Interpretation of certain words and expressions

2.—(1) In this Act, and in every written law enacted before or after 28th December 1965, the following words and expressions shall, without prejudice to anything done prior to that date, have the meanings respectively assigned to them unless there is something in the subject or context inconsistent with such construction or unless it is therein otherwise expressly provided:

...

"prescribed" means prescribed by the Act in which the word occurs or by any subsidiary legislation made thereunder and, in relation to forms, includes being set out in electronic form on an electronically accessible server (such as an internet website) that is specified in the Act or subsidiary legislation in which the word occurs;

Forms

7. Except as is otherwise expressly provided, whenever forms are prescribed, slight deviations therefrom, not affecting the substance or calculated to mislead, shall not invalidate them.

Additional provisions as to subsidiary legislation

20. The following provisions shall also apply to subsidiary legislation:

(a) authority to make subsidiary legislation shall include —

.....

(iv) authority to provide for the manner and method in which any document, record, application, permit, approval or licence may be submitted, issued or served by electronic means, or for the authentication thereof;

(b) authority to provide for fees and charges shall include authority to provide for the determination of the manner and method of payment and the reduction, waiver or refund thereof, either generally or in any particular event or case or class of cases or in the discretion of any person; and

…..

[158] Cap.1, section 20(a)(iv). This sub-paragraph was added by the Electronic Transactions Act (Cap.88).

[159] Cap.1, section 20(b). The words "the determination of the manner and method of payment and" were added by the Statutes (Miscellaneous Amendments) Act 1997(Act 7 of 1997).

4.6.6 Third, the Interpretation Act enables forms that need to be prescribed to be set out in electronic form on an electronically accessible server (such as an internet website), instead of being published in the *Gazette*.[160]

4.6.7 The Interpretation Act further provides for the electronic *Gazette.* This enables subsidiary legislation[161] to be published electronically instead of in paper form.[162]

4.6.8 In addition, these provisions are supported by the computer output provisions in sections 35 and 36 of the **Evidence Act**[163] introduced in 1996 and bolstered by the **Computer Misuse Act**[164].

4.7 Prescribed Forms

4.7.1 The law often requires prescribed forms to be used for various transactions with Government agencies. In the past, such forms were typically intended to be completed and submitted in paper form. The layout and wording of the form would be published in the Act or subsidiary legislation prescribing the form.

4.7.2 The advent of electronic transactions brought with it the possibility of providing and accepting electronic forms. This might involve providing an electronic version of a form (e.g. by e-mail or on a website) for printing and submission in paper form. Alternatively, the form might be displayed onscreen via an online terminal or a website to allow input and submission to be done electronically.[165] There would usually be no difficulty in making the onscreen display correspond in appearance to the form prescribed by legislation. In

[160] Cap.1, definition of "prescribed" in section 2(1). Amendment made by the Statutes (Miscellaneous Amendments) Act 2003 (Act 9 of 2003).
[161] Subsidiary legislation includes rules, regulations, orders, notifications, by-laws or other instruments made under any Act, with legislative effect.
[162] Cap.1, definition of *"Gazette"* in section 2(1), read with section 2(6). Amendment made by the Electronic Transactions Act (Cap.88).
[163] Cap. 97.
[164] Cap. 50A.
[165] For example, e-filing of tax returns on the IRAS website or e-polling for HDB upgrading on terminals provided by HDB.

any case, slight deviations from prescribed forms, not affecting the substance or calculated to mislead, do not invalidate the forms.[166]

4.7.3 The law already supports such transactions. Government agencies that accept the filing of documents under written law are empowered to accept the filing of such documents in the form of electronic records.[167] The Government agency may, so long as it has a general power to make subsidiary legislation, make subsidiary legislation to provide for electronic submission, issue, service and authentication of documents.[168] Further, forms that need to be prescribed can also be set out in electronic form on an electronically accessible server (such as an internet website), instead of being published in the *Gazette*, provided that the Act or subsidiary legislation requiring the form to be prescribed specifies the server or website.[169]

4.7.4 One way of providing integrated services is to enable the user to perform multiple transactions from a single point of access. The law may require different prescribed forms to be submitted for different transactions. For convenience, the user should be able to input his relevant information just once instead of having to fill in the same information repeatedly in multiple forms. An input screen catering to such multiple transactions is unlikely to resemble any of the prescribed forms required for the different transactions. Nevertheless, by using technology at the backend, the information inputted by the user can be sorted and used to "populate" all the prescribed forms for the relevant transactions. The legal requirements for prescribed forms to be used for those transactions would therefore be satisfied.

4.7.5 However, there may not be any practical reason for "populating" the prescribed forms for individual transactions at the outset. Information in electronic form can be easily routed to the relevant authorities, who can then store such information in a database and view the information whenever they require and in whatever screen layout they prefer. When a user fills in a single composite electronic

[166] Interpretation Act (Cap.1) section 7.
[167] Electronic Transactions Act (Cap.88) section 47.
[168] Cap.1, section 20(a)(iv). This sub-paragraph was added by the Electronic Transactions Act (Cap.88).
[169] Cap.1, definition of "prescribed" in section 2(1). Amendment made by the Statutes (Miscellaneous Amendments) Act 2003 (Act 9 of 2003).

form in order to perform multiple transactions, the relevant information can be routed to the relevant authorities by technology at the backend.

4.7.6 Such composite electronic forms are unlikely to resemble the paper forms prescribed for the transactions performed. They can however be prescribed as an alternative means to the prescribed paper forms[170]. Since the electronic composite form is intended for use in different transactions, some portions of the form may elicit information for one transaction that is irrelevant to other transactions. The instructions on the form can clarify which portions need to be filled for particular transactions.

4.7.7 The provision in the Interpretation Act[171] that enables forms to be prescribed by setting out in electronic form on an electronically accessible server (such as an internet website) holds a solution. In reliance on this provision, legislation governing the relevant transactions can specify the server or website where the electronic composite form can be accessed. The electronic composite form would therefore be the prescribed electronic form for that transaction. Since such an electronic form is itself a "prescribed" form, it does not need to resemble any other prescribed paper forms.[172]

4.7.8 The existing law appears to provide adequately for the circumstances discussed above.[173] Nevertheless, proposed amendments to section

[170] See footnote 18.

[171] See footnote 18.

[172] There is therefore no need to rely on section 7 of the Interpretation Act.

[173] The Electronic Transactions Model Law prepared by the Commonwealth Expert Group on E-Commerce contains a provision that makes an electronic form equivalent to a prescribed non-electronic form provided 3 requirements are satisfied: s.8. The requirements are that the form must be (a) organised in the same or substantially the same way as the prescribed form, (b) accessible to the public authority so as to be usable for future reference and (c) capable of being retained by the person to whom it is given. The provision is subject to an overarching consent requirement: s.17. The Model Law also contains a provision on "Government uses" which is broadly similar to section 47 of the ETA: s.14.

We are of the view that a provision like that in the Commonwealth model law would not be useful in Singapore. This is because section 47 already enables the Government to use electronic forms in place of prescribed forms. The 3 requirements may be overly restrictive, for example in requiring that the electronic form must be organised in the same or substantially the same way as the prescribed form. In any case, the relevant public authority can adopt any of these requirements under section 47

The provisions of the Commonwealth Model Law referred to are set out below:

47 to facilitate the use of electronic records for a wide range of government functions will also apply to facilitate use of electronic forms. **Proposed section 47(3) provides that a requirement of written law for a document to be filed is satisfied by the transmission, in the manner specified by the Government agency, of an electronic record specified by the Government agency for that purpose.**[174] (See illustration on workings of proposed section 47(3) in paragraph 4.9.5.)

"**Prescribed forms**

8. A rule of law that requires a person to provide information in a prescribed non-electronic form to another person is satisfied by the provision of the information in an electronic form that is

(a) organised in the same or substantially the same way as the prescribed non-electronic form;

(b) accessible to the other person so as to be usable for subsequent reference; and

(c) capable of being retained by the other person."

"17. (1) Nothing in this Act requires a person to use, provide or accept information in electronic form without consent, but a person's consent to do so may be inferred from the person's conduct."

(2) Despite subsection (1), the consent of a public body [use of term also used in s. 14 for government] to accept information in electronic form may not be inferred from its conduct but must be expressed by communication accessible to the public or to those most likely to communicate with it for particular purposes."

"14.(1) If a public body has power to create, collect, receive, transfer, distribute, publish, issue or otherwise deal with information and documents, it has the power to do so electronically.

(2) Subsection (1) is subject to any rule of law that expressly prohibits the use of electronic means or expressly requires them to be used in specified ways.

(3) For purposes of subsection (2), a reference to writing or signature does not in itself constitute an express prohibition of the use of electronic means.

(4) Where the public body consents to receive any information in electronic form, it may specify:

(a) the manner and format in which the information shall be communicated to it;

(b) the type or method of electronic signature required, if any;

(c) control processes and procedures to ensure integrity, security and confidentiality of the information;

(d) any other attributes for the information that are currently specified for corresponding information on paper.

(5) The requirements of subsection 7(1) [requirement for writing satisfied by information in electronic form if accessible so as to be usable for subsequent reference] and subsection (3) [information in electronic form is not given unless the information is capable of being retained by the person to whom it is given] and section 8 [prescribed forms] also apply to information described in subsection (4).

(6) A public body may make or receive payment in electronic form by any manner specified by the public body [and approved by the responsible authority]."

Section 14(5) of the Model Law is intended to provide for subsections 7(1) and (3) [writing requirements] and section 8 [prescribed forms] to supplement any additional requirements specified by Government.

[174] See Annex B.

4.8 Non-documentary Information

4.8.1 Sometimes the law merely requires that information must be furnished to a Government agency without requiring it to be in documentary form e.g. information could be furnished orally.[175]

4.8.2 Currently, section 47(1)(a) of the ETA applies only to the filing, creation and retention of *documents*. It may be convenient to extend section 47 to legal requirements for information to be furnished to a Government agency.

4.8.3 Where a provision does not specify the form in which information is to be furnished, there is probably nothing to prevent the information from being furnished in electronic form e.g. via email. Nevertheless, by extending section 47 to such information, it will make it clear that section 47(2) applies so that the Government agency can make specifications concerning the acceptance of such information in electronic form. The Government agency, of course, has to consider whether any authentication of the sender of such information is necessary.

4.8.4 We propose to extend section 47 to apply to legal requirements for information to be furnished to Government agencies, whether in documentary or other form. For this purpose, we propose to insert the words "obtain information in any form" in section 47(1)(a). In addition, proposed section 47(3) provides that a requirement of written law for information in any form to be provided is satisfied by the transmission, in the manner specified by the Government agency, of an electronic record specified by the Government agency for that purpose.[176]

4.9 Intermediaries

4.9.1 Integrated transactions may be conducted via electronic systems that are administered by a party other than the Government agency responsible for administering the relevant transaction ("an

[175] E.g. the Money–Changing and Remittance Business Act (Cap.187) s.7 requires a person to submit an application for a licence to MAS and to furnish MAS with such information as they may require; the Sand and Granite Regulations (Cap.284, Rg1) requires submission of a written application and furnishing of information to the Licensing Officer.

[176] See draft amendments to section 47 in Annex B.

intermediary") and the intermediary may process the information submitted before transmitting it to the relevant Government agency. Especially where private sector services are integrated with the delivery of government services, the intermediaries may even be private bodies or businesses.

4.9.2 The relevant law may state that a person must submit documents or provide information *to a particular Government agency or officer*.[177] As such, there may be a doubt whether such legal requirements are satisfied by filling in an electronic form on an electronic portal run by another Government or private body.

4.9.3 Some legislation, such as the Sewerage and Drainage Act (Cap.294), anticipates this issue by providing for submission of plans to "such filing authority as the Director may designate".[178] This enables the use of a filing authority for the purposes of CORENET. However, most other laws do not have such a provision.

4.9.4 Proposed section 47(3) will ensure that a wide range of requirements under written law relating to Government transactions will be satisfied by the transmission, in the manner specified by the Government agency, of electronic records specified by the Government agency for that purpose. **If a Government agency specifies the submission of a specified record via a particular electronic system, proposed section 47(3) would ensure that an electronic record submitted in accordance with those specifications satisfies the requirements of law.**[179] **This would be effective notwithstanding that such electronic system is administered by an intermediary and that the intermediary processes the information submitted before transmitting it to the relevant Government agency.**

4.9.5 For example, if Law A requires paper Form A to be submitted to Agency A, and Law B requires paper Form B to be submitted to Agency B, both Agencies A and B can specify composite Form C

[177] E.g. the Money–Changing and Remittance Business Act (Cap.187) s.7 requires a person to submit an application for a licence to MAS and to furnish MAS with such information as they may require; the Sand and Granite Regulations (Cap.284, Rg1) requires submission of a written application and furnishing of information to the Licensing Officer.
[178] Section 33.
[179] See draft amendments to section 47 in Annex B.

(which is accessible on an integrated system operated by an intermediary T) for their respective transactions under Law A and B. When an applicant completes Form C and submits it via the integrated system, pursuant to section 47(3), he will satisfy the requirements of both Law A and Law B.[180]

4.9.6 We had earlier considered whether an additional provision specifically validating the use of intermediaries would be necessary for the purposes described in this Part.[181] We do not think that such provision would be necessary in view of the operation of proposed section 47(3).

4.10 Retention of Documents

4.10.1 Under some laws, Government agencies are empowered to require persons to retain certain documents, to be produced for inspection or reference if later required.[182]

4.10.2 Many businesses and individuals adopt the practice of converting their paper records into electronic form to reap the advantages of lower storage costs (since paper records are bulky and costly to store and manage). With the adoption of electronic filing systems, records are more and more commonly created and stored in electronic form

[180] The Online Application System for Integrated Services (OASIS), available through www.Business.gov.sg, provides advice on the licences and registrations necessary to set up a business, and enables applicants to make applications to different agencies online.

[181] **Integrated transaction systems**

47A. Section 47(3) and (4) shall, for the avoidance of doubt, also apply where an electronic record, or transaction (as the case may be) referred to in either of those subsections forms part of an integrated transaction system, notwithstanding that —

(a) more than one transaction is carried out with one or more Government agencies through the generation or transmission of a single electronic record;

(b) the transactions are governed by the same or different written laws; and

(c) the transaction is processed or routed, electronically or otherwise, through an intermediary.

[182] For example, under s 199 of the Companies Act, companies are obliged to retain their accounting and other financial records for a period of 7 years. Similarly, the Income Tax Act (Cap.134) s.67. Also Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap.65A), s.37, (Retention of records by financial institutions); Securities and Futures Act (Cap.289), s.102 (Keeping of books), s.131 (Register of securities); Goods and Services Tax Act (Cap.117A), s.44 (Giving of receipts); Singapore Tourism (Cess Collection) Act (Cap.305C), s.9; Prevention of Pollution of the Sea Act (Cap.243), s.13 (Regulations requiring the keeping of cargo record books); Financial Advisers Act (Cap.110) s.45 (Accounts to be kept by licensed financial advisers).

from the point of creation, and paper copies are only printed out when required for specific purposes.

4.10.3 It is important that legal requirements should not hamper businesses and individuals from adopting efficient and cost-saving technology for records management, unless there are good reasons for rejecting such means. The need to prevent fraudulent alteration of records may be a reason in some circumstances. However, it should be recognised that paper records may not necessarily be inherently safer since technology often provides adequate or superior means of preventing such fraud in the case of electronic records.[183] Another consideration is that electronic records are subject to the risk of technological obsolescence and may become inaccessible as a result of incompatibility of the storage format with later technology. It may therefore be appropriate to demand retention in paper form for records that will be required a long time into the future, especially if timely conversion of such records to ensure accessibility with later technology cannot be assured. Government agencies would also have to consider "downstream" issues, such as, how electronically retained records can subsequently be transmitted to the Government agency for inspection, whether a printout of the retained electronic records would suffice or whether the agency is prepared to go on-site to view the records.

4.10.4 Section 9 of the ETA provides that where a rule of law requires certain records to be retained[184], the requirement is satisfied by retaining them in the form of electronic records, subject to certain conditions as to accessibility, accuracy, details of its origin, destination and time of sending and receipt.[185] This provision applies both to Government and non-government transactions. However, in the case of Government transactions, the consent of the Government agency which has supervision over the requirement for the retention of such records must have been obtained.[186] The Government agency

[183] For example, via secure audit trails and access control. Forensic analyses required to detect paper forgery may be much more complicated.
[184] See footnote 182.
[185] These requirements, based on the UNCITRAL Model Law, are intended to replicate the purposes for which documents are reproduced to be retained.
[186] IRAS has guidelines on the "Keeping of Records in Imaging System" and "Keeping Machine Sensible Records and Electronic Invoicing" (see http://www.iras.gov.sg). Application for approval must be made in writing to the Comptroller.

may also specify any additional requirements for the retention of electronic records that are subject to the jurisdiction of the Government agency.[187]

4.10.5 In recognition of the trend towards the retention of records in electronic form, and the uncertainty caused by the requirement for prior consent from Government agencies to retain records in electronic form,[188] **we propose to amend the law to make it the default position that Government agencies will accept the electronic retention of documents.** We therefore propose to delete the requirement for consent in section 9(1)(d). With this amendment, the default position for Government agencies will be consistent with that for the private sector.

4.10.6 Government agencies will continue to be able to specify additional requirements for the retention of electronic records under their purview.[189]

4.10.7 To cater to situations where there are valid concerns regarding the appropriateness of electronic retention of documents for particular purposes, **Government agencies will be able to "opt-out" of the default position. Such opt-outs will be effected by publishing an order in the *Gazette* specifying the requirement of law and the documents, records or information to which section 9 shall not apply.[190]**

4.10.8 Government agencies should, in addition, give adequate publicity to their decision to exclude section 9 in respect of a requirement for the retention of certain documents. They could, for example, publish the fact on a publicly accessible central website (e.g. the Singapore Government Online portal[191]) or their own agency website or take

[187] Section 9(4) ETA.
[188] There have been industry complaints that many Government agencies when asked for consent for electronic retention, will either not comment or say vaguely and verbally (but not in writing) that they have no objection. This means that businesses cannot safely convert to electronic document management systems as they do not know whether they will fall foul of Government requirements later on.
[189] See Annex B, new section 9(1)(d) which is based on existing section 9(4)(b).
[190] See Annex B. Section 9(4)(b).
[191] www.gov.sg.

even more proactive steps to ensure that persons affected are aware of their requirements if necessary.

4.10.9 These amendments will enable businesses and individuals to confidently proceed to retain their records in electronic form, unless there is an order stating that section 9 does not apply to specified requirements of law in respect of specified documents, records or information.

4.10.10 We propose to retain both sections 9 and 47 although there would be some duplication in relation to the electronic retention of documents for Government purposes. These provisions should be allowed to work together since they address different aspects of the issue.

4.10.11 Section 9 is a general provision applying to both Government and private sector requirements. It stipulates requirements as to accessibility, accuracy and identification in relation to the retention of the documents.[192] It will apply to Government transactions unless the relevant Government agency has opted out of the provision.

4.10.12 We propose to retain the references to the retention of documents in section 47 for consistency with other Government functions governed by that provision. Since this is the principal section governing e-Government initiatives, it should, in our view, be as comprehensive as possible. Proposed section 47(3) applies where the Government agency has specified the documents and the manner of transmission. Section 47(1) deals with the flipside of the issue, that is, it is primarily concerned with empowering Government agencies to use electronic records for their functions, if they decide to do so. **We only propose a slight amendment to existing section 47(3)** [193] **to ensure that the default position with opt-out under section 9 will prevail.**

4.11 Originals

4.11.1 The law often requires the production of original documents to support applications to Government agencies. Government agencies

[192] These requirements, based on the UNCITRAL Model Law, are intended to replicate the purposes for which documents are reproduced to be retained.

[193] Existing section 47(3) will br renumbered as section 47(4). We propose to add the words "Subject to section 9 and 9A" at the beginning of the provision. See Annex B.

usually require original documents to be produced in order to verify certain information contained in that document. In most cases, the documents required pertain to Government records or certificates or licences issued by the Government. For example, one way of proving one's status for registration of citizenship by birth is to produce a birth certificate with the name of the child.[194] In other cases however, documents originating from other sources may be required. For example, a document duly authenticated to be the original document containing or recording testimony in a foreign court may be required for the purposes of extradition proceedings.[195]

4.11.2 In some situations, it may be convenient to accept an electronic copy of an original paper document. For example, the paper documents may be located in another country and the holder may not wish to let the document out of his possession.[196] The acceptance of electronic originals would cut down the need for face-to-face transactions to verify documents, thus paving the way for more Government services to be provided electronically from end-to-end.

4.11.3 As appropriate technology becomes available to safeguard the integrity of electronic documents, more and more organisations (governmental and non-governmental) are adopting electronic means of storing information and creating records. In such a case, there may no longer be a paper original since the record is created and stored in electronic form. It may be convenient for a Government agency requiring the production of original records to accept the production of such records in electronic form.

4.11.4 We envisage that in the future it may be less crucial for Government agencies to require paper originals for verification as Government agencies now frequently obtain information directly from source. For example, IRAS obtains pay information directly from certain employers, information on charitable donations to certain organisations is provided directly by the organisations, and information on dividend payments are obtained directly from the Central Depository.

[194] National Registration Act (Cap.201) section 12.
[195] Extradition Act (Cap.103) section 42(2).
[196] Indeed Canada was exploring the adoption of electronic imaging and transmission for immigration applications because often the applicants and their original documents are located outside Canada.

4.11.5 In this discussion, for convenience, we use the term "electronic originals" to refer to both electronic copies of paper originals as well as originals created in electronic form. The ETA currently does not contain any provision on the acceptance of electronic originals.

4.11.6 However, in some cases, such provision may not be necessary since the terms of the relevant provision of law imposing the requirement for the production of an original can already be read to admit originals created in electronic form.

4.11.7 In other cases, a piecemeal approach has been taken. Pursuant to the existing legislative framework which enables provisions to be made for the acceptance and authentication of documents by subsidiary legislation,[197] necessary legislative provisions have been made in Singapore as particular agencies adopt new electronic processes to facilitate the production of documents by electronic means.

4.11.8 Section 47 does not currently extend to the acceptance of original documents in electronic form.[198] In order to provide a more comprehensive framework, **we propose to amend section 47 to allow Government agencies to accept electronic originals.**

4.11.9 In Part 5.11, we discuss the adoption of a general provision on originals[199]. In addition, we discuss in Part 4.12 other issues related to achieving functional equivalence between the production of information in electronic form and conventional means, which apply to both government and private transactions.

4.12 General

Multiple specific provisions?

4.12.1 A survey of other jurisdictions indicates that they have adopted provisions relating to the production and retention of documents and

[197] ETA s.47 and Interpretation Act s.20.
[198] Although the reference to the "filing of documents" in section 47 could possibly include originals in some circumstances, it would probably not extend to the production of originals for on-the-spot verification. Speaking of "filing" of electronic originals raises complications since transmission of the "original" to the Government agency's computer system would actually involve the transmission of a copy.
[199] See proposed section 9A in Annex B.

information in various ways. Some jurisdictions have followed the UNCITRAL formulation fairly closely. For example, Canada and Ireland have both the provision on electronic originals and the provision on retention of documents.[200] However, in addition, Canada also has provisions on providing information in writing[201] and in specific form[202].

4.12.2 The Australian Commonwealth has not adopted any provision on originals as such. The "production of documents" was thought to be a more appropriate term because the concept of an original document is not used in their laws.[203] Instead, their law contains a number of provisions dealing with specific situations in which documents are required to be retained or produced, namely: requirements for the production of documents in paper or similar form[204], recording of information in writing[205], retention of written documents[206], and retention of electronic communications[207].

4.12.3 New Zealand has a similar approach to Australia. Their law deals specifically with legal requirements to record information in writing[208], to give information in writing[209], to retain documents or information that is in paper or non-electronic form[210], to retain information that is in electronic form[211], to produce information that is in paper or non-electronic form[212], to produce information that is in electronic form[213], to provide access to information that is in non-electronic form[214], to provide access to information that is in

[200] Canadian Uniform Electronic Commerce Act ss. 11 and 13, and Irish Electronic Commerce Act 2000 ss.17 and 18.
[201] Canadian Uniform Electronic Commerce Act s. 8
[202] Canadian Uniform Electronic Commerce Act s. 9
[203] Revised Explanatory Memorandum on the Electronic Transactions Bill 1999 accessed at http://scaleplus.law.gov.au/html/ems/0/1999/0/0642410364.htm.
[204] Australian Commonwealth Electronic Transactions Act 1999 s.11.
[205] Australian Commonwealth Electronic Transactions Act 1999 s.12(1).
[206] Australian Commonwealth Electronic Transactions Act 1999 s.12(2) and (3).
[207] Australian Commonwealth Electronic Transactions Act 1999 s.12(4) and (5).
[208] New Zealand Electronic Transactions Act 2002 s.19.
[209] New Zealand Electronic Transactions Act 2002 s.20.
[210] New Zealand Electronic Transactions Act 2002 s.25.
[211] New Zealand Electronic Transactions Act 2002 s.26.
[212] New Zealand Electronic Transactions Act 2002 s.28.
[213] New Zealand Electronic Transactions Act 2002 s.29.
[214] New Zealand Electronic Transactions Act 2002 s.30.

electronic form[215] and to compare a document with an original document.[216]

4.12.4 The Australian and New Zealand laws deal with each kind of transaction separately and with specificity. Their approach highlights the fact that articles 8 and 10 of the UNCITRAL Model Law[217] cover a wide range of transactions and there is some overlap between the kinds of transactions that these articles apply to.

4.12.5 Some Singapore laws expressly refer to the requirement to produce "original" documents.[218] Other laws may simply require that a certain document be produced. Although the word "original" may not have been used, it may be clear from the context that a particular document is required and not a mere copy of it. Therefore section 9 (on retention of documents) and a provision on originals based on the UNCITRAL Model (if adopted) could apply simultaneously to the same transaction and document.

4.12.6 Such overlap may give rise to confusion if the two provisions have inconsistent criteria for the acceptance of information in electronic form. Further, inconsistencies as to whether consent is required from the party to whom the document is to be produced or for whom the document is retained could be problematic.[219]

4.12.7 **We therefore propose that, whether there is a single provision on originals or a number of specific provisions on different situations in which electronic communications are used, the requirements as to consent or opting out and compliance with additional technical requirements should be consistent across**

[215] New Zealand Electronic Transactions Act 2002 s.31.
[216] New Zealand Electronic Transactions Act 2002 s.32.
[217] i.e. respectively relating to originals and retention of documents, on which our proposed section 9A and our existing section 9 are based.
[218] E.g. Insurance (Accounts and Statements) Regulations 2004 requires lodgment of an "original" actuary's report with the Monetary Authority of Singapore (regulation 11); Moneylenders Rules requires moneylenders to keep "in a file in which he shall place in consecutive order the original memoranda of all loans made by him in that year" (rule 12); Land Surveyors Rules require the submission of "original" field notes, calculations and plans by examination candidates (rule 12). Originals are also widely required in relation to evidence and procedure in court proceedings. We do not deal with issues of evidence and procedure in court proceedings as these are specifically dealt with under the Evidence Act and Rules of Court (in connection with the electronic filing system).
[219] See further paragraphs 4.12.10 to 4.12.16 on requirements for consent in relation to provisions on production and retention of documents and originals.

such provisions. This is why proposed section 9A of the ETA adopts provisions on opting out and compliance with technical requirements that mirror the proposed amendments to section 9 of the ETA.[220]

4.12.8 **In the Singapore context, it may not be necessary to have multiple provisions dealing specifically with each kind of transaction.** This is because section 47 of the ETA already provides comprehensively for Government agencies to accept electronic means of carrying out its functions. Proposed section 47(3) ensures that the use of electronic means specified by Government agencies to carry out such transactions satisfies the legal requirements for such transactions.[221] As earlier noted, most legal requirements on the production or retention of documents or information relate to Government transactions. With the exclusion of negotiable instruments, documents of title and land transactions, there are probably no such legal requirements that apply between private parties.

4.12.9 **To minimise repetition and overlap between the provisions of the ETA, we propose to adopt a single provision on electronic originals instead of many separate provisions to cater to the different situations in which electronic communications are used.** However, we propose to adopt the provision on electronic originals despite the overlap with sections 9 and 47 for the reasons discussed in this Part.

Consent and additional technical requirements

4.12.10 Most of the jurisdictions surveyed expressly provide that their electronic transactions laws do not compel anyone to use or accept electronic technology without their consent, though consent may be inferred from conduct.[222] Such consent may be given subject to conditions regarding the form of the information or the means by

[220] See Annex B. Proposed sections 9A(1)(c) and 9(4) mirror section 9(1)(d) and 9(4)(b) respectively.
[221] See discussion in Part 1.4.
[222] Canadian Uniform Electronic Commerce Act s.5, Irish Electronic Commerce Act 2000 s.24 and New Zealand Electronic Transactions Act 2002 s.16. The Australian Commonwealth Electronic Transactions Act 1999 does not have a general consent provision, but there are consent requirements in each section in Division 2 of Part 2 of the Act, except section 12 (relating to retention).

which the information is produced, sent, received, processed, stored or displayed.[223]

4.12.11 The position with regard to acceptance of information in electronic form by the Government differs from jurisdiction to jurisdiction. The Australian Commonwealth requires Commonwealth entities to accept electronic communications, except in the case of transactions that have been specifically excluded by the legislation.[224] New Zealand requires consent to accept the electronic form to be obtained in relation to legal requirements to give information in writing[225] and to produce[226] or provide access[227] to information that is in paper or other non-electronic form.

4.12.12 On the other hand, the provisions on retention of documents or information in the jurisdictions surveyed, except Ireland, do not contain any requirement for the consent of the person for whom they are retained.[228] Perhaps it is thought that it is sufficient for the requirement for consent to come into play only when the information retained has to be produced to another party.[229] The New Zealand provision on the legal requirement to compare a document with an original document[230] also does not contain any provision on consent.

4.12.13 In addition to the requirement for consent to accept electronic communications, any additional technical requirements of Government agencies accepting such communications must also be complied with.[231] Section 16 of the New Zealand Act applies this without distinction between Government and non-Government bodies.[232]

[223] New Zealand Electronic Transactions Act 2002 s.16.
[224] Australian Commonwealth Electronic Transactions Act 1999 s.11.
[225] New Zealand Electronic Transactions Act 2002 Section 20
[226] New Zealand Electronic Transactions Act 2002 Section 27
[227] New Zealand Electronic Transactions Act 2002 Section 30
[228] Canadian Uniform Electronic Commerce Act s.13, New Zealand Electronic Transactions Act 2002 s.16, Australian Commonwealth Electronic Transactions Act 1999 s.12 c.f Irish Electronic Commerce Act 2000 s.18.
[229] i.e. the consent requirements in one of the provisions on production of documents will then apply.
[230] Section 32.
[231] Canadian Uniform Electronic Commerce Act s.8, 9 and 11, Irish Electronic Commerce Act 2000 s.17 and 18, and Australian Commonwealth Electronic Transactions Act 1999 s.11. Section 16 of the New Zealand Electronic Transactions Act 2002 applies this to provision without distinction between Government and non-Government bodies.
[232] New Zealand Electronic Transactions Act 2002.

4.12.14 We have proposed to amend section 9 to provide that, as a default position, Government agencies will accept the retention of documents in electronic form unless the requirement for retention of that document has been expressly excluded by order published in the *Gazette*. [233] This is intended to give greater certainty to individuals and businesses seeking to convert their paper records into electronic form.

4.12.15 Bearing in mind the difficulties that may be encountered as a result of inconsistent consent requirements, **we propose to adopt a similar opt-out provision[234] in relation to the provision on electronic originals (or, if specific provisions on different situations in which electronic communications may be used are preferred, in relation to each of those provisions)**. This requirement for Government agencies to opt-out is similar in approach to that in Australia.[235]

4.12.16 Existing section 9 of the ETA (on retention of electronic records) contains a provision requiring compliance with any additional requirements specified by the Government agency with purview over the retention requirement.[236] We proposed to retain this provision with modifications.[237] **We propose to adopt a similar provision on compliance with technical requirements of the relevant Government agency in the provision on electronic originals (or if specific provisions on different situations in which electronic communications may be used are preferred, in relation to each of those provisions).[238]**

4.13 The adoption of provisions for functional equivalence in relation to the production of information in electronic form raises various issues:

Q10. Do you have any comments on the proposed amendments to section 9 of the ETA in Annex B?

[233] See proposed section 9(4)(b) in Annex B and Part 4.10.
[234] See footnote 233.
[235] See proposed section 9A(4) in Annex B.
[236] Existing section 9(4)(b) of the ETA.
[237] Part 4.10. See proposed section 9(1)(d) in Annex B.
[238] Part 4.11. See proposed section 9A(1)(c) in Annex B.

Q11. Do you have any comments on the proposed amendments to section 47 of the ETA in Annex B?

Q12. Should Singapore adopt a single provision on electronic originals or provide specifically for different situations in which electronic communications may be used as a functional equivalent of paper or other non-electronic forms?[239] (See paragraphs 4.12.1 to 4.12.9, especially paragraphs 4.12.8 and 4.12.9).

Q13. Should consent to accept electronic originals be required? In this respect, should there be any distinction between Government agencies and private persons or entities, and if yes, what differences should there be? For example, should Government agencies be presumed to accept electronic originals unless they have opted out of doing so, as proposed in section 9A(4) in Annex B? Would your views differ if, instead of a single provision on electronic originals, there are specific provisions on the use of electronic communications in different situations? (See paragraphs 4.12.10 to 4.12.12).

Q14. Proposed sections 9 and 9A of the ETA[240] require compliance with any additional technical requirements as to form and procedure that Government agencies may have in relation to the acceptance of electronic originals. Should there be express requirements to comply with such additional technical requirements in the case where the intended recipient of electronic originals is not a Government agency? Would your views differ if, instead of a single provision on electronic originals, there are specific provisions on the use of electronic communications in different situations? (See paragraphs 4.12.13 to 4.12.16)

[239] See Australian Commonwealth Electronic Transactions Act 1999 and New Zealand Electronic Transactions Act 2002. Also Canadian Uniform Electronic Commerce Act.
[240] See draft sections 9(1)(d) and 9A(1)(c) in Annex B.

PART 5
UNCITRAL ELECTRONIC CONTRACTS CONVENTION AND RELATED ISSUES

5.1 The draft UNCITRAL Convention on the Use of Electronic Communications in International Contracts (the Convention)[241], is expected to be considered and possibly finalised by UNCITRAL at its 38th session scheduled to be held in Vienna from 4 to 15 July 2005. The draft Convention is available on the UNCITRAL website at www.uncitral.org. The Convention is intended to govern international commercial contracts.[242]

5.2 If the Convention is widely adopted by other countries, it will set an international standard. In view of Singapore's trading interests, it would be in Singapore's interest to have laws which are consistent with such international standards.

5.3 If Singapore accedes to the Convention, it is likely that same regime applicable under the Convention will be adopted for all contractual transactions whether local or international. The Electronic Transactions Act will therefore have to be amended for consistency with the provisions of the Convention. This is because it would be confusing to have 2 separate legal regimes for local and international contracts, especially since it is often difficult to determine in the case of electronic transactions whether one is contracting with a local or foreign party.

---

[241] The draft Convention and related documents are available at the UNCITRAL website (www.uncitral.org), under Working Group IV. The current version of the draft Convention is A/CN.9/571.

[242] Article 1(1) provides that the Convention applies "to the use of electronic communications in connection with the formation or performance of a contract [or agreement] between parties whose places of business are in different States". The word "formation" is to be interpreted widely to include all contracting stages, including negotiations and invitations to make offers. A/CN.9/571, paragraph 15.

Article 2(1) excludes certain types of transactions, in particular:

> "(a) Contracts concluded for personal, family or household purposes;
>
> (b) (i) Transactions on a regulated exchange, (ii) foreign exchange transactions; (iii) inter-bank payment systems, inter-bank payment agreements or clearance and settlement systems relating to securities or other financial assets or instruments; (iv) the transfer of security rights in, sale, loan or holding of or agreement to repurchase securities or other financial assets or instruments held with an intermediary."

Article 2(2) excludes application to "bills of exchange, promissory notes, consignment notes, bills of lading, warehouse receipts or any transferable document or instrument that entitles the bearer or beneficiary to claim the delivery of goods or the payment of a sum of money".

5.4 In Stage I of the *Joint IDA-AGC Public Consultation on the Review of the Electronic Transactions Act: Electronic Contracting Issues* (LRRD No.1/2004),[243] conducted in February to April 2004, we had highlighted the main changes and issues which would arise in relation to electronic contracting if the provisions of the draft Convention (as it then stood)[244] were to be adopted. Since then, the UNCITRAL Working Group has met twice[245] to continue its work on the Convention and the draft of the Convention has undergone various modifications.

5.5 In this Part, we will highlight the changes that have been made to the draft Convention and discuss the implications of those changes for electronic contracts. This Part also discusses issues that may arise from the adoption of the Convention provisions in the ETA. It is necessary to consider to what extent it would be appropriate to apply the provisions of the Convention, which is restricted in its application to the context of international contracts, to domestic contracts and non-contractual transactions[246].

5.6 The following topics are discussed in this Part:

- Consent and Variation (Part 5.7)
- Legal Recognition of Electronic Communications (Part 5.8)
- Writing Requirement (Part 5.9)
- Electronic Signatures (Part 5.10)
- Provision of Originals (Part 5.11)
- Time and Place of Despatch and Receipt (Part 5.12)
- Invitation to Make Offers (Part 5.13)
- Automated Message Systems (Part 5.14)
- Error in Electronic Communications (Part 5.15)
- Applicability of the Convention (Part 5.16)

5.7 Consent and Variation

5.7.1 Article 3 of the draft UNCITRAL Convention provides that "parties may exclude the application of the Convention or derogate from or

[243] Available on the AGC website (www.agc.gov.sg), under Publications.
[244] A/CN.9/WG.IV/WP.103.
[245] 43rd session (New York, 15-19 March 2004), 44th session (Vienna, 11-22 October 2004).
[246] e.g. Government transactions.

vary the effect of any of its provisions". Article 8(2) provides that "nothing in the Convention requires a party to use or accept electronic communications, but a party's agreement to do so may be inferred from the party's conduct". There has been no change to these provisions of the Convention. These provisions preserve party autonomy in relation to contracts to which the Convention applies.

5.7.2 In LRRD No.1/2004[247], we explored whether to adopt a consent provision in the ETA based on article 8(2). We also noted that section 5 of the ETA provides for variation by agreement of any provision of Part II[248] or IV[249] of the ETA and considered whether to amend or replace the provision in view of overlap with other provisions making specific sections apply subject to agreement otherwise and the need for mandatory requirements which should not be open to variation by agreement of parties, and also whether a variation provision would be necessary if there is a consent provision.

5.7.3 All of the respondents[250] agreed that parties should generally have the freedom not to use electronic means to contract. The majority of respondents felt that an express provision would help to clarify this point. Two respondents however were of the view that the common law already provides adequately for this. Under the common law, a party need not accept a contractual offer if he does not consent to it. The common law, it was pointed out, has a detailed system of rules and standards[251] to ensure consent.

5.7.4 The respondents[252] also generally agreed that parties should not be permitted to adopt standards that are lower than the minimum requirements for the legal recognition of electronic communications

[247] Consultation Paper for Stage 1 of the *Joint IDA-AGC Public Consultation on Review of the Electronic Transactions Act: Electronic Contracting Issues*, Part 2.1.
[248] On Electronic Records and Signatures generally and, in particular, containing provisions on the legal recognition of electronic records, the requirement for writing, electronic signatures, and the retention of electronic records.
[249] On Electronic Contracts and, in particular, regarding the formation and validity of contracts, effectiveness between parties, attribution, acknowledgment of receipt and time and place of dispatch and receipt.
[250] To the Stage 1 Consultation Paper. See footnote 247.
[251] e.g. rules relating to consent, intention to create legal relations, mistake, etc.
[252] See footnote 250.

in the ETA[253] and other rules of law. One respondent however cautioned that the requirements of such minimum standards should be made clear.

5.7.5 The prevailing view within the UNCITRAL Working Group was that the right of a party to derogate from the application of the draft Convention should not be restricted. It was noted that the draft Convention was only intended to provide functional equivalence in order to meet general form requirements and that it did not affect mandatory rules that required, for instance, the use of specific methods of authentication in a particular context.[254]

5.7.6 As the ETA extends beyond contracts to include other transactions**,** it is necessary to consider whether consent and variation provisions should extend to other transactions.[255]

5.8 Legal Recognition of Electronic Communications

5.8.1 Article 8 provides for the legal recognition of electronic communications as follows:

> "1. A communication or a contract shall not be denied validity or enforceability on the sole ground that it is in the form of an electronic communication.".

5.8.2 This provision, read with the definitions of "communication"[256] and "electronic communication"[257] cover both (a) contracts formed by the exchange of electronic communications and (b) the general use of electronic means to convey a statement, declaration, demand, notice or request in connection with a contract.

[253] e.g. conditions applicable to the retention of electronic records under section 9 of the ETA. (See discussion in Part 4.10.) Also proposed section 9A on provision of originals. (See discussion in Part 4.11.) c.f. the reliability requirement discussed in Part 5.10.
[254] A/CN.9/571, paragraph 76.
[255] See discussion on consent in relation to section 9 (retention of electronic records) and proposed section 9A (Provision of originals) in Part 4, paragraphs 4.12.10 to 4.12.16.
[256] "communication" means any statement, declaration, demand, notice or request, including an offer and acceptance of an offer, that the parties are required to make in connection with the formation or performance of a contract.
[257] "electronic communication" means any communication that the parties make by means of data messages.

5.8.3 This provision is consistent with both sections 6 and 12 of the ETA. In LRRD No.1/2004,[258] we consulted on whether references to "declaration, demand, notice or request" should be added to section 12 of the ETA for consistency. The majority of respondents felt that this would be useful for clarity. Some respondents however felt it was unnecessary as "declaration of intent or other statement" covers all of the listed documents. **On balance, we do not think that any amendment is required to sections 6 and 12 of the ETA.**

5.9 Writing Requirement

5.9.1 Article 9 provides for electronic communications to satisfy legal requirements for writing as follows:

> "1. Nothing in this Convention requires a communication or a contract to be made or evidenced in any particular form.
>
> 2. Where the law requires that a communication or a contract should be in writing, or provides consequences for the absence of a writing, that requirement is met by an electronic communication if the information contained therein is accessible so as to be usable for subsequent reference.".

5.9.2 The words "the law" in the provision has the same meaning as in corresponding provisions of the UNCITRAL Model Law on Electronic Commerce and refer to rules based on statute, regulation or judicial precedent.[259]

5.9.3 This provision is consistent with section 7 of the ETA.

5.10 Electronic Signatures

5.10.1 In LRRD No.1/2004[260] we noted that the provision on the recognition of electronic signatures in article 9 of the draft UNCITRAL Convention (as it then stood)[261] included 2 variants. Variant A was based on article 7 of the UNCITRAL Model Law on

[258] See footnote 247
[259] A/CN.9/571, paragraph 125.
[260] See footnote 247
[261] A/CN.9/WG.IV/WP.103.

Electronic Commerce, while variant B was based on article 6, paragraph 3 of the UNCITRAL Model Law on Electronic Signatures.[262]

5.10.2 The Working Group decided in favour of retaining variant A only.[263] Paragraphs 4 and 5 of article 9[264] have been deleted. Article 9(3) of the draft Convention now provides for electronic signatures as follows:

> "3. Where the law requires that a communication or a contract[265] should be signed by a party, or provides consequences for the absence of a signature, that requirement is met in relation to an electronic communication[266] if:
>
> (a) A method is used to identify the party and to indicate that party's approval of the information contained in the electronic communication; and
>
> (b) That method is as reliable as appropriate to the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement.".

[262] A/CN.9/546, paragraph 48, see footnote 241.
[263] A/CN.9/546, paragraph 54-57, see footnote 241.
[264] Article 9(4) and (5) of the draft UNCITRAL Convention (from the 49th session of Working Group IV), based on article 6 of the Model Law on Electronic Signatures , read as follows:

"4. An electronic signature is considered to be reliable for the purposes of satisfying the requirements referred to in paragraph 3 of this article if:
(a) The signature creation data are, within the context in which they are used, linked to the signatory and no other person;
(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;
(c) Any alteration to the electronic signature, made after the time of signing, is detectable; and
(d) Where the purpose of the legal requirement for a signature is to provide assurances as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.
5. Paragraph 4 of this article does not limit the ability of any person:
(a) To establish in any other way, for the purposes of satisfying the requirement referred to in paragraph 3 of this article, the reliability of an electronic signature;
(b) To adduce evidence of the non-reliability of an electronic signature.".

[265] The words "declaration, demand, notice or request that the parties are required to make or choose to make in connection with a contract" have been deleted. See paragraph 5.8.2.
[266] Reference to "data massage" has been replaced by "electronic communication".

Definition of electronic signature

5.10.3 Article 9(3)(a) of the draft Convention lays down general criteria for functional equivalence between handwritten signatures and electronic signatures.[267] Article 9(3)(a) defines an electronic signature as "a method ... used to identify the party *and* to indicate that party's approval of the information contained in the electronic communication" (italics added). This conjunctive requirement may be read to mean that only an electronic signature that fulfils both the function of identification of the party *as well as* the function of indicating that party's approval of the information contained in the electronic communication meets that legal requirement of a signature in relation to an electronic communication.[268]

5.10.4 There may be instances where the law requires a signature that does not fulfil the function of indicating the signing party's approval of the information contained in the electronic communication. For example, in the case of requirements of law for notarisation of a document by a notary or attestation by a commissioner for oath, it is not the intention of the law to require the notary or commissioner, by signing, to indicate his approval of the information contained in the electronic communication. The signature of the notary or commissioner merely identifies the notary or commissioner, and associates the notary or commissioner with the contents of the document, but does not indicate the approval by the notary or commissioner of the information contained in the document. Similarly, laws may require the execution of a document to be

[267] Paragraph 3(a) of article 9 is based on article 7, paragraph 1(a) of the UNICTRAL Model Law on Electronic Commerce 1996. Article 7 of the UNCITRAL Model Law on Electronic Commerce states:

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

[268] It should be noted that under paragraph 3 of article 9, which originated from article 7, paragraph 1 of the UNCITRAL Model Law on Electronic Commerce, the mere signing of an electronic communication by means of a functional equivalent of a handwritten signature is not intended, in and of itself, to confer legal validity on the data message. Whether an electronic communication that fulfilled the requirement of a signature has legal validity is to be settled under the law applicable outside the draft convention. See paragraph 61 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996).

witnessed by a witness, who is required to append his signature to that document. The signature of the witness merely identifies the witness and associates the witness with the contents of the document witnessed, but does not indicate the approval by the witness of the information contained in the document. In each of the examples above, the notary or commissioner and the witness, by signing, can at most be said to "approve" the words in the *jurat*[269] and not all the information contained in the document.

5.10.5 By contrast, "electronic signature" is defined in the ETA 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[270] *or* approving the electronic record" (italics added). The use of the word "or" makes the stated functions of the signature disjunctive. Therefore, the definition recognises electronic signatures that fulfill only one of the functions, even if it does not fulfill both of the functions, e.g. an electronic signature that authenticates the electronic record but does not indicate approval of the electronic record.

5.10.6 As article 9(3)(a) may prevent electronic signatures that are not intended to fulfill the function of indicating the signor's approval of the information contained in the electronic communication to satisfy a requirement of law for a signature, Singapore has submitted a comment to the UNCITRAL Secretariat requesting UNCITRAL to consider amending article 9(3)(a) to recognise that electronic signatures are sometimes required by law only for the purpose of identifying the person signing ("the signor") and associating the information with the signor, but not necessarily to indicate the signor's "approval" of the information contained in the electronic communication. The full text of the comment submitted to UNCITRAL is set out at Annex C.

[269] i.e. a memorandum usually appearing in legal documents above the signature of the notary, commissioner or witness, stating that that notary, commissioner or witness witnessed the signor of the document append his signature to the document.

[270] Although there is no explicit reference to the "identification" function in the definition, it is implicit in the definition.

Q15. Do you agree that the definition of an electronic signature should not require such a signature to fulfill both an identification as well as an approval function?

Reliability requirement

5.10.7 Article 9(3)(b) of the draft Convention contains a requirement that the method of signing must be "as reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement" in order for the electronic signature to be legally valid.

5.10.8 This means that the parties to the electronic communication or contract are not able to know with certainty *ex ante*[271] whether the electronic signature used will be upheld by a court or other trier of fact as "appropriately reliable" and therefore not be denied legal validity, until after a legal dispute arises subsequently. It also means that even if there was *no dispute* about the identity of the person signing or the fact of signing (i.e. no dispute as to authenticity of the electronic signature), a court or trier of fact may still rule that the electronic signature was not appropriately reliable, and therefore invalidate the entire contract.

5.10.9 Such a provision will potentially have serious practical implications for electronic commerce:

(a) It will create uncertainty in electronic transactions because whether a signature method is appropriately reliable and hence not be denied legal validity will be determined *ex post*[272] by the court or trier of fact, and not *ex ante* by the parties. Although parties can exercise party autonomy by agreeing on a signature method, it remains that the parties' agreement is only one of the factors taken into consideration by the court or trier of fact.[273] Even if the parties were satisfied at the outset as to the reliability

[271] i.e. at the outset e.g. when signing.
[272] i.e. after the event
[273] This was explicitly noted at paragraph 60 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996), which states, "However, a possible agreement between originators and addressees of data messages as to the use of a method of authentication is not conclusive evidence of whether that method is reliable or not."

of the signature method, a court or trier of fact may rule otherwise.

(b) It could be used to the detriment of the very class of persons that the legal requirements for signature are intended to protect. A party could try to invalidate his own electronic signature as being insufficiently reliable, in order to invalidate a contract, where it is convenient to him. This would be to the detriment of the other party relying on the signor's signature. This provision then risks becoming a trap for the unwary or a loophole for the unscrupulous.

(c) It may be an impediment to electronic commerce. It will add to business costs if users feel compelled to use more sophisticated and costly technology to ensure that the reliability requirement is satisfied. Conversely, such uncertainty and additional costs may even discourage the use of electronic transactions.

5.10.10 This "reliability requirement" has its origins in article 7, paragraph 1(b) of the UNCITRAL Model Law on Electronic Commerce 1996. In the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures 2001, it was noted that article 7 of the UNCITRAL Model Law on Electronic Commerce creates uncertainty as the determination of appropriately sufficient reliability can only be made *ex post* by a court or other trier of fact. In order to create more certainty *ex ante*, article 6, paragraph 3 of the UNCITRAL Model Law on Electronic Signatures 2001 was introduced.[274]

5.10.11 It is noted that there is no such "reliability requirement" for the legal validity of handwritten signatures (or any of the other marks on paper that may constitute a signature at law). Common law does not impose any form requirement on signatures. A person can sign by marking a cross "X" on a document. A person can also sign by a machine that prints his name on a document. Both the cross "X" and machine-printed name are legally valid signatures, though questions of proof may arise. In each case, it is a matter of proof whether the purported signor did in fact sign in that manner and intended thereby

[274] Paragraph 118 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures 2001.

to sign the document. In order to establish the signature's function of linking the signor with the signed document, the context of the signing will always have to be demonstrated, whether the signature is on paper or electronic.

5.10.12 It is not the form of the signature, but the proven link between the signature and the purported signor based on the context, that gives the signature its legal effect. In commercial transactions, the person relying on a signature always takes the risk that the signature is not genuine, so he evaluates the risk that the signature is not genuine and protects himself accordingly.[275] The risk analysis will of course include the cost of having the signature made more reliable and the cost of its being not genuine. So a history of dealings with the purported signor, or a low-value transaction, may persuade someone to rely on a signature that would not be satisfactory if it were from a stranger or for a high value transaction. These precautions and judgments are not a matter of law but a matter of prudence. That is, a party may not feel comfortable about relying on a signature in the form of a cross "X", but that is a judgment by that party as a matter of prudence, and not a matter of law, as the signature in the form of a cross "X" is fully valid as a signature at law. We are of the view that this analysis applies equally where electronic commercial transactions and electronic signatures are concerned.

5.10.13 Singapore has submitted a comment to the UNCITRAL Secretariat proposing to delete paragraph 3(b) of article 9 of the draft Convention (A/CN.9/577), to achieve functional equivalence between handwritten signatures and electronic signatures, and to avoid the unintended difficulties that would be created by the inclusion of the general legal "reliability requirement" in paragraph 3(b). The full text of the comment submitted to UNCITRAL is set out at Annex C.

5.10.14 The ETA does not contain such a reliability requirement for electronic signatures to satisfy requirements of law for signatures. Instead section 8 of the ETA underlines that a flexible approach will be taken in the manner of proving an electronic signature.[276] If the

[275] This may involve checking the signature against known genuine versions of it, or getting the signature witnessed, notarized or guaranteed by a bank, etc.
[276] See footnote 277.

reliability requirement in the draft Convention is adopted, section 8[277] of the ETA would need to be amended. The regime suggested by the reliability requirement in the draft Convention more closely resembles the regime relating to secure electronic signatures under section 17.[278]

5.10.15 In our view, there should not be any general reliability requirement imposed in a provision providing for the functional equivalence of electronic signatures and handwritten signatures.[279]

5.10.16 Signature requirements under the law exist mainly in relation to specialised transactions (such as negotiable instruments or land transactions which have been excluded from the ETA) and transactions with Government agencies (which, under existing law[280] generally have power to stipulate alternative requirements). Where, after due consideration of the policy and purposes of specific requirements for a signature in a particular law, a relevant authority is satisfied that additional reliability requirements for electronic signatures would be desirable, such requirements can be prescribed in the relevant law or (in cases outside the ambit of the ETA) a court can impose such requirements as a matter of interpretation of the legal requirement[281]. It would be clearer to specify the standard of

[277] **Electronic signatures**

8.-(1) Where a rule of law requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law.

(2) An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a party, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of such party.".

[278] **Secure electronic signatures**

17. If, through the application of a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that an electronic signature was, at the time it was made ---

(a) unique to the person using it;
(b) capable of identifying such person;
(c) created in a manner or using a means under the sole control of the person using it; and
(d) 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,

such signature shall be treated as a secure electronic signature.

[279] i.e. section 8 of the ETA.

[280] i.e. section 47 of the ETA.

[281] The High Court in *SM Integrated Transware Pte Ltd v Schenker Singapore (Pte) Ltd* [2005] SGHC 58 decided that, notwithstanding the exclusion (under section 4 of the ETA) of contracts for

reliability required of electronic signatures in relation to particular requirements of law rather than to rely on a general reliability requirement.

5.10.17 If Singapore accedes to the Convention, such additional requirements would have to be declared under article 18(2) of the Convention (see Part 5.16).

Q16. Do you agree that a general provision providing for the functional equivalence of electronic signatures to handwritten signatures (e.g. section 8) should not contain any reliability requirement?

Q17. Should any laws imposing a signature requirement be clarified by prescribing the requirements as to reliability that should apply to electronic signatures? If yes, please state the legal requirement (e.g. Civil Law Act, section 6) and describe the standard that should be required of electronic signatures in order to satisfy that legal requirement.

5.11 Provision of Originals

5.11.1 Article 9(4), (5) and (6) of the Convention provides as follows:

> "4. Where the law requires that a communication or a contract to be presented or retained in its original form, or provides consequences for the absence of an original, that requirement is met in relation to an electronic communication if:
>
> (a) There exists a reliable assurance as to the integrity of the information it contains from the time when it was first generated in its final form, as an electronic communication or otherwise; and
>
> (b) Where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.
>
> 5. For the purposes of paragraph 4(a):

the disposition of immovable property from the application of section 8 of the ETA, a court could decide whether, as a matter of common law, an electronic signature satisfied a legal requirement for signature under section 6 of the Civil Law Act in respect of a contract for lease.

> (a) The criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and
>
> (b) The standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.
>
> [6. Paragraphs 4 and 5 do not apply where a rule of law or the agreement between the parties requires a party to present certain original documents for the purpose of claiming payment under a letter of credit, a bank guarantee or a similar instrument.]".

5.11.2 This provision was added to the Convention to support the effective use of electronic means to conclude arbitration agreements since the enforcement of an arbitral award and the referral of parties to arbitration under articles II and IV of the 1958 New York Convention require a party relying on the arbitration agreement to produce its original or duly certified copy thereof. Nevertheless the Working Group noted that the usefulness of this provision extends beyond arbitration.[282]

5.11.3 The provision does not however address the issue of singularity, which is relevant to documents of title and negotiable instruments. The general agreement of the Working Group seems to be that the issue should not be addressed in the Convention, but in future UNCITRAL work on negotiable instruments. Article 2(2) excludes various kinds of documents of title and negotiable instruments from the application of the Convention.[283] Article 9(6), which excludes letters of credit, bank guarantees and similar instruments from the application of article 9(4) and (5), is still under review by UNCITRAL. As an alternative, it was proposed that the draft convention give States the possibility to exclude the application of article 9(4) and (5) by declarations made under draft article 18.[284]

[282] A/CN.9/571, paragraphs 129, 130 and 132.
[283] See paragraph 5.16.3. A/CN.9/571, paragraph 156.
[284] See paragraph 5.16.5. A/CN.9/571, paragraph 138.

5.11.4 Article 9(4) and (5) is essentially the same as the provisions in article 8 of the UNCITRAL Model Law on Electronic Commerce.[285] The ETA does not currently contain any provision on electronic originals.

5.11.5 The issue of electronic originals was previously discussed in the Stage I consultation paper on *Review of Electronic Transactions Act: Electronic Contracting Issues*.[286] There was little enthusiasm for such a provision amongst the respondents to the consultation as it was felt that, for commercial purposes, private parties could be left to make their own arrangements for the acceptance of originals. One respondent however advocated that legislation would be useful in promoting the development and acceptance of technology for the use of electronic originals.[287]

5.11.6 The related issue of provision for electronic documents of title and negotiable instruments was discussed in the Stage II consultation paper on *Review of the Electronic Transactions Act: Exclusions under section 4*.[288] Here again, there was little enthusiasm for such a provision amongst the respondents. In the case of negotiable instruments, it was felt that there is currently no demand for such provision because electronic cheques are not widely used. In the case of documents of title, the respondents generally advocated caution. In both cases, it was felt that legislation should only be made in tandem with the development of international norms.

5.11.7 Although we recognise that technology and practice in this area is still evolving, we note that provisions on electronic originals based on article 8 of the UNCITRAL Model Law on Electronic Commerce are widely accepted in other jurisdictions.[289] Such a provision could

[285] Except for drafting amendments substituting references to "communication or contract" in view of the limited ambit of the draft Convention.
[286] LRRD 1/2004, Part 7.2.
[287] Response by Mr Kenneth Lim of Crimson Logic, available on www.ida.gov.sg.
[288] LRRD 2/2004, Parts 4 (Negotiable Instruments) and 9 (Documents of Title, including discussion of the carriage of goods provision in articles 16 and 17 of the UN Model Law on E-Commerce).
[289] Canadian Uniform Electronic Commerce Act s.11, Irish Electronic Commerce Act 2000 s.17, Hong Kong Electronic Transactions Ordinance s.7. See also the US E-Sign Act s.101(d)(1) and (3). Section 32 of the New Zealand Electronic Commerce Act which relates to the "legal requirement to compare a document with an original document" however only adopts the requirement of reasonable assurance of integrity. Section 28 of the New Zealand Act relating to the requirement to provide information or to produce information in paper form adopts those criteria and could apply to the provision of originals. The Australian Commonwealth Electronic Transactions Act 1999 does not contain any provision on originals. Such issues are instead dealt with by section 11 and 12 of the

provide useful guidance on this nascent issue and facilitate the adoption of technology for electronic originals as it is developed. Further, if the draft Convention, which adopts a similar provision on electronic originals is widely adopted by other countries, it will set an international standard.

5.11.8 This provision does not prevent parties from agreeing to additional requirements in relation to the acceptance of originals. Further, with a consent provision, no one will be forced to accept electronic originals and private parties can continue to agree on arrangements to accept originals.[290]

5.11.9 In view of the general sentiment obtained from our public consultations, however, we agree that negotiable instruments and documents of title should continue to be excluded from the application of the ETA under section 4. Specific legislation may be made for such instruments when appropriate.

5.11.10 A further reason for the exclusion of negotiable instruments and documents of title is that the provision of originals does not address the issue of singularity. For similar reasons, it has been suggested that letters of credit and bank guarantees should also be considered for exclusion from the ambit of the provision on originals.[291]

5.11.11 With the exclusion of negotiable instruments and documents of title from the application of the ETA, we realize that a provision on electronic originals would have little application, except in relation to the requirement for originals by Government agencies. Nevertheless, we think that it would still be appropriate to adopt such a provision for consistency with legislation in other jurisdictions internationally and to complement our legislative framework in relation to the electronic retention of documents.[292]

Australian Act, relating to production and retention of documents, which also adopt criteria based on the UNCITRAL Model Law.

[290] See paragraph 5.7 on consent and variation.

[291] See paragraph 5.11.3.

[292] See Part 4.10 on the proposed amendments to section 9 of the ETA.

5.11.12 **We therefore propose to adopt a provision on electronic originals in the ETA.** (Please see proposed section 9A in Annex B.)[293]

Criteria for acceptance of electronic originals

5.11.13 Despite the different formulations adopted by the different jurisdictions surveyed[294], they have all adopted variations of the criteria of reliable assurance of integrity[295] (or accuracy) and accessibility[296] in provisions on electronic originals and similar provisions. "Accessibility", which covers both the usability of the record for subsequent reference and its capability of being retained by the person to whom the record is provided, is an extension of the requirement in the UNCITRAL Model Law which merely provides that the information must be capable of being displayed to the recipient.[297] It may however be questioned whether the capability of retention and re-use should be a requirement where the original is required only for the purposes of a once-off validation.

5.11.14 Where the provisions deal more specifically with particular situations, as in Australia and New Zealand, the criteria have been modified as appropriate for the specific situations. In New Zealand, where there are separate provisions in relation to paper documents being converted to electronic form and records that were created in electronic form, the requirements are basically the same for both forms of records except that in the case of conversion of an electronic record into a paper document, there is a requirement to notify the recipient if the integrity of the document cannot be assured and to produce the electronic record if requested to do so.[298] In the case of electronic communications that have to be transmitted, there

[293] See also Part 4.11 on originals in the context of e-Government.
[294] Canada, Australia, New Zealand and Ireland.
[295] "Integrity" means that the information has remained complete and unaltered, apart from any changes that arise in the normal course of communication, storage or display. The standard of reliability is to be assessed in relation to the document and in the light of all the circumstances.
[296] Canadian Uniform Electronic Commerce Act s.11, Irish Electronic Commerce Act 2000 s.17, Hong Kong Electronic Transactions Ordinance s.7. See also the US E-Sign Act s.101(d)(1) and (3). Section 32 of the New Zealand Electronic Commerce Act which relates to the "legal requirement to compare a document with an original document" however only adopts the requirement of reasonable assurance of integrity. However section 28 of the New Zealand Act relating to the requirement to provide information or to produce information in paper form adopts those criteria and could apply to the provision of originals.
[297] Hong Kong adopted the UNCITRAL formulation i.e. capability of display.
[298] New Zealand Electronic Transactions Act 2002 s. 29 and 31

is also a requirement for the record to identify the sender and recipient and time when it was sent and received.[299]

5.11.15 We note that some jurisdictions have added qualifications to the criteria. For example, in Australia, the requirement for accessibility has to be complied with "at the time the communication was sent" (in the provision on production of documents)[300] or "at the time of commencement of the retention of the information" (in the provision on retention of electronic communications) [301], and only to the extent that "it was reasonable to expect" that the information would be so accessible at that time.[302] Further, the provisions on retention of documents or information in Australia are limited to requirements for retention "for a particular period" and the requirement to retain additional information as to the origin, destination and time or sending and receipt continues only during that period.[303]

Q18. What difficulties or benefits do you foresee if the provisions of article 9(4) and (5) of the draft convention (relating to originals) are adopted in the ETA?

Q19. Do you have any comments on proposed section 9A in Annex B? Do you agree with the criteria for acceptance of electronic originals in proposed section 9A(1) and (2) in Annex B?

5.11.16 The adoption of a provision in the production of originals raises other issues. These are further discussed in Part 4.[304]

5.12 Time and Place of Despatch and Receipt

5.12.1 Article 10 of the Convention now reads:

> "1. The time of dispatch of an electronic communication[305] is the time when it leaves an information system under the

[299] New Zealand Electronic Transactions Act 2002 s. 27
[300] Australian Commonwealth Electronic Transactions Act 1999 s.11.
[301] Australian Commonwealth Electronic Transactions Act 1999 s.12(4).
[302] Also Irish Electronic Commerce Act 2000 s. 17(2)(c) and 18(2)(c).
[303] Australian Commonwealth Electronic Transactions Act 1999 s.12(4)(c)
[304] Paragraphs 4.12.1 to 4.12.9 discuss whether to have a single provision on originals or many specific provisions. Paragraphs 4.12.10 to 4.12.16 discuss consent and additional technical requirements.
[305] References to "data messages" have been replaced by references to "electronic communications".

control of the originator[306] or of the party who sent it on behalf of the originator or, if the electronic communication has not left an information system under the control of the originator or of the party who sent it on behalf of the originator, at the time when the electronic communication is received.

2. The time of receipt of an electronic communication is the time when it becomes capable of being retrieved by the addressee at an electronic address designated by the addressee. The time of receipt of an electronic communication at another electronic address is the time when it becomes capable of being retrieved by the addressee at that address and the addressee becomes aware that the electronic communication has been sent to that address. An electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the addressee's electronic address.

3. An electronic communication is deemed to be dispatched at the place where the originator has its place of business and is deemed to be received at the place where the addressee has its place of business, as determined in accordance with article 6.

4. Paragraph 2 of this article applies notwithstanding that the place where the information system supporting an electronic address is located may be different from the place where the electronic communication is deemed to be received under paragraph 3 of this article.".

5.12.2 Section 15 of the ETA provides that an electronic record is **despatched** when "it enters an information system outside the control of the originator or the person who sent the electronic record on behalf of the originator".[307]

5.12.3 The Convention changes this to the time it "leaves an information system under the control of the originator or of the party who sent it on behalf of the originator".

[306] The words in square brackets that were deleted referred to entry into an information system outside the control of the originator or of the person who sent the data message on behalf of the originator.
[307] Section 15(1)

5.12.4 As regards **receipt** of an electronic record, a number of separate rules apply under section 15. If an information system has been designated for receipt of the record, the electronic record is received when it "enters the designated information system".

5.12.5 The Convention changes this to the time when it becomes capable of being retrieved by the addressee at an electronic address designated by the addressee". The concept of a "designated information system" has been replaced by the concept of an "electronic address".[308]

5.12.6 Under section 15, if the electronic records are sent to another information system that was not designated by the addressee, receipt occurs when it is retrieved by the addressee.[309] If no information system was designated by the addressee, *receipt* occurs when the electronic record enters the information system of the addressee.[310]

5.12.7 The Convention changes the time of receipt of an electronic communication "at another electronic address of the addressee" to the time "when it becomes capable of being retrieved by the addressee at that address and the addressee becomes aware that the

[308] The Working Group agreed on the understanding that this term is not limited to e-mail addresses, but is open to future technological development. It was also stated that, as used in the draft provision, the term referred to "a portion or location in an information system that a person uses for receiving electronic messages". The Working Group however preferred not to include a definition in the draft Convention, leaving the concept to be elucidated in any explanatory notes or official commentary to the draft convention. A/CN.9/571

[309] Section 15(2)(a)

[310] Section 15(2)(b).

Some jurisdictions have adopted a rule whereby, in the absence of a designated information system, a message is deemed to be received when the addressee *became aware* of the data message and the message was *capable of being retrieved*. Canada provides a presumption that an electronic record is received only when the addressee becomes aware of the record *and* it is accessible by the recipient: UECA section 23(2)(b). The Australian Act and New Zealand Act provide that the time of receipt is the time when the electronic communication comes to the attention of the addressee. The Report of the Australian Electronic Commerce Expert Group to the Attorney-General on Electronic Commerce: Building the Legal Framework, paras 2.15.15 and 2.15.17, noted the need to address the issue of whether an electronic record is communicated only if it is actually read by the recipient.

Such a rule is more equitable than holding an addressee bound by a message sent to an information system that the addressee could not reasonably expect would be used in the context of its dealings with the originator or for the purpose for which the message was sent. On the other hand, it may be potentially unfair for the addressee unilaterally to have power to determine whether and when receipt would occur. The test is also inherently more uncertain since it will often depend on factors within the knowledge of the recipient or the ISP alone. It may also be difficult to obtain evidence from an ISP based outside the jurisdiction of the court. The test of entry into a particular information system is, on the other hand, technically easier to prove.

electronic communication has been sent to that address". There is therefore no longer any distinction whether the addressee has or has not designated an electronic address for receipt; the same rules will apply as long as communication is sent to an electronic address that the addressee has not designated. Mere entry into the addressee's information system or capability of retrieval are no longer sufficient; The communication must be capable of being retrieved **and** the addressee must be aware that the electronic communication has been sent.

5.12.8 An electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the addressee's electronic address. This presumption is rebutted if it is shown that the communication was not in fact retrievable. Specific examples discussed by the Working Group were situations where the communication arrived outside of office hours or where security or other devices would prevent the communication from being retrieved.[311]

5.12.9 As regards the **deemed place of dispatch and the deemed place of receipt** of an electronic communication, article 10(3) of the draft Convention provides similarly to section 15(4) of the ETA. Article 10(3) makes reference to article 6[312], which clarifies the meaning of place of business. Compared with section 15(5) of the ETA, article 6 of the draft Convention contains further clarifications on the provisions on location of the parties.

[311] A/CN.9/571, paragraphs 159 and 160.

[312] Article 6. Location of the parties.

1. For the purposes of this Convention, a party's place of business is presumed to be the location indicated by that party, unless another party demonstrates that the party making the indication does not have a place of business at that location.

2. If a party has not indicated a place of business and has more than one place of business, then [, subject to paragraph 1 of this article,] the place of business for the purposes of this Convention is that which has the closest relationship to the relevant contract, having regard to the circumstances known to or contemplated by the parties at any time before or at the conclusion of the contract.

3. If a natural person does not have a place of business, reference is to be made to the person's habitual residence.

4. A location is not a place of business merely because that is: (a) where equipment and technology supporting an information system used by a party in connection with the formation of a contract are located; or (b) where the information system may be accessed by other parties.

5. The sole fact that a party makes use of a domain name or electronic mail address connected to a specific country does not create a presumption that its place of business is located in that country.

5.12.10 Article 6(1) presumes that a party's place of business is the "location indicated by that party, unless another party demonstrates that the party making the indication does not have a place of business at that location".[313] The Convention does not impose any requirement that parties must disclose their identity or place of business, but article 7[314] expressly provides that the Convention does not affect the application of any rule of law requiring such disclosure.[315] Article 6(2), which relates to the situation where a party had more than one place of business, is similar to section 15(5)(a) of the ETA, except that it clarifies that regard is to be had "to the circumstances known to or contemplated by the parties at any time before or at the conclusion of the contract".[316] Article 6(3) notably applies only in respect of a natural person who does not have a place of business. Section 15(5)(b), read with section 15(5)(c)[317], by contrast, extends to bodies corporate.[318]

5.12.11 Article 6 further clarifies that a "location is not a place of business merely because that is (a) where equipment and technology supporting an information system used by a party in connection with the formation of a contract are located; or (b) where the information

[313] The Working Group regarded this provision to be useful for companies with several places of business, with more than one having connections with a specific contract. This provision would allow the company to indicate one of its places of business, with the consequence that the indication cannot be challenged unless the company did not have a place of business at the location indicated. A/CN.9/571, paragraph 98.

[314] Article 7. Information requirements.

Nothing in this Convention affects the application of any rule of law that may require the parties to disclose their identities, places of business or other information, or relieves a party from the legal consequences of making inaccurate or false statements in that regard.

[315] Many European States impose such disclosure requirements on online service providers as a matter of consumer protection.

[316] The main purpose of this provision is to provide a default rule where a party having more than one place of business fails to indicate the place of business for that particular transaction. A/CN.9/571, paragraph 100. For cases where a party had only one place of business and did not disclose it, the definition in article 4(h) ("Place of business" means any place where a party maintains a non-transitory establishment to pursue an economic activity other than the temporary provision of goods or services out of a specific location.) already provides an answer.

[317] Section 15(5)(c) provides that, in relation to a body corporate, "usual place of residence" means the place where it is incorporated or otherwise legally constituted.

[318] The draft Convention refers to "habitual residence" instead of "usual place of residence" because it is intended only to apply to natural persons. The Working Group felt it was unwise to alter the wording which is common in uniform law conventions. It acknowledged that there might be legal entities, so-called "virtual companies", whose establishment might not meet all the requirements of the definition of "place of business" in article 4(h). A/CN.9/571, paragraph 103.

system may be accessed by other parties".[319] It also provides that the "sole fact that a party makes use of a domain name or electronic mail address connected to a specific country does not create a presumption that its place of business is located in that country".[320]

5.12.12 Article 10(4) of the draft Convention is similar to section 15(3) of the ETA, except for consequential changes as a result of the adoption of the concept of "electronic address" and the term "electronic communication".

5.12.13 Various concerns were raised in respect of the earlier version of this provision of the Convention by respondents to LRRD No.1/2004[321]. A major concern was the uncertainty which arose from the provision that the presumption that the data message was capable of being retrieved would be rebutted if "it was unreasonable for the originator to have chosen that particular information system for sending the data message". This reference to unreasonableness has been removed from the current Convention draft. In the case of receipt at an electronic address that was not designated by the addressee, there is an additional requirement that the addressee must actually be aware that the communication has been sent. The adoption of the new concept of "electronic address" also helps to clarify the uncertainties that previously related to the term "information system" of that party or under their control. The concern about communications received after office hours or when the addressee does not in fact have access to the communication have also been addressed by the fact that the presumption concerning receipt is rebutted if it is shown that the communication was not in fact retrievable.[322]

[319] Article 6(4). The Working Group decided not to provide for "virtual companies" as the matter at this early stage was better left to the elaboration of emerging jurisprudence. A/CN.9/571, paragraph 107. See also footnote 318.

[320] Article 6(5). This only prevents domain name from being the sole factor in determining the location of a party. It does not prevent a court or arbitrator from taking into account the domain name as a possible element, among others, to determine a party's location, where appropriate. A/CN.9/571, paragraph 113.

[321] Part 5, see footnote 247

[322] See Part 5.12, especially paragraphs 5.12.5, 5.12.7 and 5.12.8. Other concerns raised about hijacked mail, denial of service attacks and wrong clock settings would all be matters to be proved to show that a communication was not capable of being retrieved or was not sent at the purported time, and are beyond the scope of the provision.

5.12.14 These default rules help to provide greater certainty as to the time and place of dispatch and receipt of electronic communications. Their adoption will however entail changes to the existing law under section 15 of the ETA.

Q20. What difficulties or benefits do you foresee if the provisions of article 10 of the draft Convention (relating to time and place of dispatch and receipt of electronic communications) are adopted in the ETA?

5.13 Invitation to Make Offers

5.13.1 Article 11[323] of Convention makes it the default rule that proposals made to the world at large are to be considered as an invitation to make offers. The provision preserves party autonomy by stating that the default rule is subject to clear indication of "the intention of the party making the proposal to be bound in case of acceptance". There has been no change to the provision since we consulted on it in Stage 1 of the ETA Review[324].

5.13.2 Respondents who agreed to this provision favoured it because it would give certainty to such transactions. Those who were not in favour of this provision preferred that the rules of common law should continue to apply.

5.13.3 This provision provides greater certainty as to whether proposals made to the world at large are binding. As the ETA does not contain any provision on this issue, the position in Singapore law has to be decided in each case based on common law principles.

Q21. What difficulties or benefits do you foresee if the provisions of article 11 of the draft Convention (relating to invitation to make offers) are adopted in the ETA?

5.14 Automated Message Systems

5.14.1 The provision on automated message systems, now in article 12 of the Convention, reads:

[323] This was previously article 12 of draft Convention, A/CN.9/WG.IV/WP.103.
[324] LRRD No.1/2004, paragraph 4.2.

> "A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability on the sole ground that no natural person reviewed each of the individual actions carried out by the systems or the resulting agreement."

5.14.2 The provision has only undergone minor drafting amendments. The term "automated message system" is used instead of "automated information system". The term is defined to mean "a computer program or an electronic or other automated means used to initiate an action or respond to data messages or performances in whole or in part, without review or intervention by a person each time an action is initiated or a response is generated by the system".[325] The term "person" is clarified by referring to "natural person".

5.14.3 This provision will facilitate the use of automatic message systems[326] as it makes it explicit that contracts formed by the interaction of an automated message system and an individual, or by the interaction of automated information systems, will not be denied validity or enforceability on the sole ground that no person reviewed each of the individual actions carried out by such systems or the resulting agreement.

Q22. What difficulties or benefits do you foresee if the provisions of article 12 of the draft Convention (relating to automated message systems) are adopted in the ETA?

5.15 Error in Electronic Communications

5.15.1 Article 14 of the Convention provides as follows:

> 1. Where a natural person makes an input error in an electronic communication exchanged with the automated message system of another party and the automated message system does not provide the person with an opportunity to correct the error, that person, or the party on whose behalf that person was

[325] Article 4(g) c.f definition of the term "information system" in article 4(f) as "a system for generating, sending, receiving, storing or otherwise processing data messages.

[326] E.g. reply slips on orders on Amazon.com, online travel insurance acknowledgements when users purchase insurance online.

> acting, has the right to withdraw the electronic communication in which the input error was made if:
>
> (a) the person, or the party on whose behalf that person was acting, notifies the other party of the error as soon as possible after having learned of the error and indicates that he or she made an error in the electronic communication;
>
> (b) the person, or the party on whose behalf that person was acting, takes reasonable steps, including steps that conform to the other party's instructions, to return the goods or services received, if any, as a result of the error or, if instructed to do so, to destroy the goods or services; and
>
> (c) the person, or the party on whose behalf that person was acting, has not used or received any material benefit or value from the goods or services, if any, received from the other party.
>
> 2. Nothing in this article affects the application of any rule of law that may govern the consequences of any errors made during the formation or performance of the type of contract in question other than an input error that occurs in the circumstances referred to in paragraph 1.

5.15.2 This issue was previously discussed in LRRD No.1/2004.[327] Most of the respondents to the consultation supported such a provision. One respondent voiced a concern that it is difficult to define "error". Others were concerned about regulatory burdens and the fettering of party autonomy. These concerns appear to be met by the current draft of the provision.

5.15.3 The provision has been amended to refer to "input" error. This clarifies that the provision applies only to errors relating to inputting wrong data, as opposed to other kinds of error such as misunderstanding of the terms of the contract or simply poor business judgment.

[327] Part 6.5, see footnote 247.

5.15.4 Further, the provision applies only if "the automated message system does not provide the person with an opportunity to correct the error". As most online systems would provide an opportunity to correct errors, [328] this provision would not affect such cases.

5.15.5 In other words, this provision is intended to cover a limited problem relating to the use of electronic communications. It would complement the common law of mistake[329] by balancing the need for certainty in commercial relationships and the need to protect consumers from unfair trade practices. It provides a fair basis for the exercise of the right of withdrawal[330] and would also tend to limit abuses by parties acting in bad faith. The provision "gives online merchants a way of giving themselves a good deal of security against allegations of mistake, and encourages good business practices in everybody's interests".[331]

Q23. What difficulties or benefits do you foresee if the provisions of article 14 of the Convention (relating to Error in Electronic Communication) are adopted in the ETA?

5.16 Applicability of the Convention

5.16.1 The Convention applies "to the use of electronic communications in connection with the formation or performance of a contract [or agreement] between parties whose places of business are in different States".[332] The word "formation" is to be interpreted widely to include all contracting stages, including negotiations and invitations to make offers.

[328] E.g the provision of an opportunity to confirm the order or to return and correct one's input.

[329] Under the common law doctrine of mistake which applies under Singapore law, a mistake is immaterial unless it is fundamental i.e. it results in a complete difference in substance between what the mistaken party bargained for and what the contract purports. It is likely that a court would allow the apparent contract to stand unless, on the facts, it must have been obvious to the other party that the person had made a mistake.

[330] The prevailing view of the Working Group was that the possibility to withdraw only the vitiated part of the communication was implicit in the right to withdraw the entire communication. It was decided however that the provision should not confer a right to vary the agreement. A/CN.9.571, paragraphs 194 and 196.

[331] Annotations to the Canadian Uniform Electronic Commerce Act. The provision was inspired by Canadian legislation e.g. section 22 of the Canadian Uniform Electronic Commerce Act.

[332] Article 1(1).

5.16.2 Article 2(1) excludes certain types of transactions, in particular:

> "(a) Contracts concluded for personal, family or household purposes;
>
> (b)(i) Transactions on a regulated exchange, (ii) foreign exchange transactions; (iii) inter-bank payment systems, inter-bank payment agreements or clearance and settlement systems relating to securities or other financial assets or instruments; (iv) the transfer of security rights in, sale, loan or holding of or agreement to repurchase securities or other financial assets or instruments held with an intermediary.".

5.16.3 Article 2(2) excludes application to "bills of exchange, promissory notes, consignment notes, bills of lading, warehouse receipts or any transferable document or instrument that entitles the bearer or beneficiary to claim the delivery of goods or the payment of a sum of money".

5.16.4 The following exclusions were deleted from article 2(2), as they were regarded as territory-specific issues that should be better dealt with at State level:[333]

> "(b) Contracts that create or transfer rights in immovable property, except for rental rights;
>
> (c) Contracts requiring by law the involvement of courts, public authorities or professions exercising public authority;[334]
>
> (d) Contracts for suretyship granted by, and on collateral securities furnished by, persons acting for purposes outside their trade, business or profession;
>
> (e) Contracts governed by family law or by the law of succession.".

5.16.5 An exclusion from article 9(4) and (5) where a rule of law or the agreement between the parties requires a party to present certain

[333] A/CN.9/571, paragraph 65.

[334] It was stated that this provision might have the undesirable effect of hindering the international development of electronic public procurement. Another difficulty was the reference to "tribunals" might be read to encompass arbitral bodies. A/CN.9/571, paragraph 65.

original documents for the purpose of claiming payment under a letter or credit, a bank guarantee or a similar instrument is still under consideration by UNCITRAL. As an alternative to such an exclusion, it was proposed that the Convention could give States the possibility to make such an exclusion by declaration under article 18.

5.16.6 Article 18(1) allows States to declare that the Convention will apply only to:

> "(a) When the States referred to in article 1, paragraph 1 are Contracting States to this Convention;
>
> (b) When the rules of private international law lead to the application of the law of a Contracting State; or
>
> (c) When the parties have agreed that it applies.".

5.16.7 Article 18(2) allows States to exclude matters from the scope of the Convention by declaration in accordance with article 20[335] in relation to declarations under articles 17(1) (Effect on territorial units), 18 (1) and (2) and 19(2), (3) and (4) (Communications exchanged under other international conventions).[336] It was noted, for example, that article 9 of the Convention would generally apply to any form requirements under the applicable law. Public policy rules contained in domestic law barring the use of electronic communications were to be dealt with either as exclusions under article 2 or by means of declarations of exclusions under draft article 18.

5.16.8 Section 4(1) of the ETA currently excludes Parts II and IV of the Act from applying to any rule of law requiring writing or signature in any of the following matters:

> "(a) the creation or execution of a will;
>
> (b) negotiable instruments;
>
> (c) the creation, performance or enforcement of an indenture, declaration of trust or power of attorney with the exception of constructive and resulting trusts;

[335] Article 20 relates to the procedure and effects of declarations.

[336] Such declarations may be made at any time and not only at the time of the deposit of its instrument of ratification, acceptance, approval or accession. A/CN.9/571, paragraph 32.

(d) any contract for the sale or other disposition of immovable property, or any interest in such property;

(e) the conveyance of immovable property or the transfer of any interest in immovable property;

(f) documents of title.".

5.16.9 Some of the exclusions under section 4 of the ETA correspond to exclusions under article 2 of the Convention, namely, the exclusions in article 2(2) correspond to the exclusion for negotiable instruments and documents of title in section 4(b) and (f) respectively. **The other exclusions in section 4 do not correspond to any exclusion under article 2 of the Convention. Those other exclusions, if they are to be retained in relation to the Convention, will have to be excluded by declaration under article 18(2).**

5.16.10 **It will also be necessary to make declarations with respect to provisions that impose any requirements for the acceptance of electronic communications which differ from the requirements under the Convention.** For example, if Government agencies impose additional technical or procedural specifications or any exclusions in relation to the acceptance of electronic communications (as provided for under section 9(4)(b) or 47(2) of the ETA, or proposed section 9(1)(d), 9(4)(b), 9A(1)(c) or 9A(4)) these additional specifications or exclusions will have to be declared insofar as they may affect contracts governed by the Convention.

5.16.11 It is also timely to review the legal requirements for writing, signature, retention of documents and originals under our law, to consider whether the rules for functional equivalence of electronic communications under the Convention are appropriate for the purposes of those legal requirements. For example, does an electronic signature adequately serve the purposes of section 6 of the Civil Law Act[337], or should there be specifications as to the standard

[337] Section 6 of the Civil Law Act provides:

Contracts which must be evidenced in writing

6. No action shall be brought against —

(*a*) any executor or administrator upon any special promise to answer damages out of his own estate;

(*b*) any defendant upon any special promise to answer for the debt, default or miscarriage of another person;

(*c*) any person upon any agreement made upon consideration of marriage;

of reliability that an electronic signature must meet to serve as a valid signature for the purposes of that section? If any additional requirements are to be applied for the recognition of electronic signatures for the purposes of such legal requirements, it will be necessary to declare those additional requirements under the Convention insofar as they may affect contracts governed by the Convention.

5.16.12 A further issue for consideration is whether Singapore should adopt any of the possible limitations to the applicability of the Convention mentioned in article 18(1). The imposition of such limitations would significantly restrict the applicability of the Convention. **Such limitations would seem to be unnecessary if we decide to align our law with that under the Convention. The ETA is for the most part already consistent with many of the provisions of the Convention. In most cases where there are differences, we propose to align the ETA to the Convention for consistency in the law applicable to domestic and international contracts, as well as other transactions.**

Q24.	What exclusions from the applicability of the Convention do you propose in the context of Singapore? Please specify legislative provisions affected where relevant. (See paragraphs 5.16.9 to 5.16.11)
Q25.	Do you agree that Singapore should not adopt any of the limitations in article 18(1)? (See paragraph 5.16.12)

5.17 Extension to Non-Contractual Transactions

Provisions in Part IV of ETA

5.17.1 Part IV of the ETA is entitled "ELECTRONIC CONTRACTS". The provisions in that Part are arguably limited in their application to contractual transactions. Some of the provisions, by reason of their

(*d*) any person upon any contract for the sale or other disposition of immovable property, or any interest in such property; or

(*e*) any person upon any agreement that is not to be performed within the space of one year from the making thereof,

unless the promise or agreement upon which such action is brought, or some memorandum or note thereof, is in writing and signed by the party to be charged therewith or some other person lawfully authorised by him.

subject matter, can only apply to contracts e.g. section 11 which relates to formation and validity of contracts.

5.17.2 In the case of some other provisions, there is no intrinsic reason why they cannot apply to non-contractual transactions as well e.g. provisions relating to attribution (section 13), acknowledgement of receipt (section 14) and time and place of dispatch and receipt (section 15)[338]. Indeed, we note that in the Australian Electronic Transactions Act, provisions on time and place of dispatch and receipt of electronic communications and on attribution of electronic communications are not limited to contractual transactions.

5.17.3 **We propose that the provisions relating to attribution, acknowledgement of receipt and time and place of dispatch and receipt in Part IV of the ETA should be allowed to apply to non-contractual transactions as well.** There does not seem to be any need to extend section 12 (relating to effectiveness of an electronic record, declaration of intent or other statement between parties) to non-contractual transactions since section 6 (on legal recognition of electronic records) already applies.

Provisions of UNCITRAL Convention

5.17.4 The provisions relating to legal recognition of electronic records[339], requirement for writing[340] and electronic signatures[341] in the UNCITRAL Convention already have counterparts in the ETA[342] that apply generally and are not limited to contractual transactions. There is no reason why these provisions should now be so restricted even if the provisions in the ETA are to be aligned with the UNCITRAL Convention.

5.17.5 Similarly there is no reason to limit the provision on originals[343] to contractual provisions. Indeed, as pointed out, with the proposed exclusion of various types of contractual transactions from the ambit of this provision, its remaining area for application would largely

[338] See also Part 5.12 on article 10 of the UNCITRAL Convention.
[339] Article 8, see Part 5.8.
[340] Article 9, see Part 5.9.
[341] Article 9(3), see Part 5.10.
[342] i.e. sections 6, 7 and 8 respectively.
[343] Article 9(4), (5) and (6), see Part 5.11.

consist of non-contractual transactions such as government transactions. Notably, the related provision on retention of electronic records (section 9) in the ETA is not limited to contractual transactions.

5.17.6 It is also necessary to consider whether the consent and variation provisions[344] should apply to non-contractual transactions, and if so whether any modifications are necessary. Consent in relation to section 9 (retention of electronic records) and proposed section 9A (provision of originals) are discussed in paragraphs 4.12.10 to 4.12.16.

5.17.7 The provisions on invitation to make offers[345], automated message systems[346] and error in electronic communications[347] are, by their nature, relevant only to contractual transactions.

Q26. Should sections 13, 14 and 15 in Part IV of the ETA be allowed to apply to non-contractual transactions? (See paragraphs 5.17.1 to 5.17.3)
Q27. Do you have any comments on whether any of the provisions of the Convention should apply to non-contractual transactions? (See paragraphs 5.17.4 to 5.17.7)

[344] See Part 5.7.
[345] Article 11, See Part 5.13.
[346] Article 12, see Part 5.14.
[347] Article 14, see Part 5.15.

ANNEX A

ELECTRONIC TRANSACTIONS ACT
(CHAPTER 88, SECTIONS 42 AND 61)

ELECTRONIC TRANSACTIONS (CERTIFICATION AUTHORITY) REGULATIONS

[10th February 1999]

PART I

PRELIMINARY

Citation

1. These Regulations may be cited as the Electronic Transactions (Certification Authority) Regulations.

Definitions

2. In these Regulations, unless the context otherwise requires —

"licence" means a licence granted under these Regulations;

"subscriber identity verification method" means the method used to verify and authenticate the identity of a subscriber;

"trusted person" means any person who has —

(a) direct responsibilities for the day-to-day operations, security and performance of those business activities that are regulated under the Act or these Regulations in respect of a certification authority; or

(b) duties directly involving the issuance, renewal, suspension, revocation of certificates (including the identification of any person requesting a certificate from a licensed certification authority), creation of private keys or administration of a certification authority's computing facilities.

PART II

LICENSING OFCERTIFICATION AUTHORITIES

Application to be licensed certification authority

3. —(1) Every application to be a licensed certification authority shall be made in such form and manner as the Controller may, from time to time, determine and shall be supported by such information as the Controller may require.

(2) The Controller may require the applicant to furnish such additional information as are necessary in support of the application.

(3) The Controller may allow applications for renewal of licences to be submitted in the form of electronic records subject to such requirements as the Controller may impose.

(4) A licence shall be subject to such conditions, restrictions and limitations as the Controller may, from time to time, determine.

Period of validity of licence
4. A licence shall be valid for a period of one year or such other longer period as the Controller may allow.

Renewal of licence
5. —(1) Regulation 3 shall apply to an application for renewal of a licence as it applies to a fresh application for a licence.
(2) A certification authority shall submit an application for the renewal of its licence no later than 3 months before the expiry of its licence.
(3) If the certification authority has no intention to renew its licence, the certification authority shall —
(a) inform the Controller in writing no later than 3 months before the expiry of the licence;
(b) inform all its subscribers in writing no later than 2 months before the expiry of the licence; and
(c) advertise such intention in such daily newspaper and in such manner as the Controller may determine, no later than 2 months before the expiry of the licence.

Licence fees
6. —(1) An application fee of $5,000 shall be payable to the Controller on every application for the grant or renewal of a licence to be a licensed certification authority.
(2) If the application referred to in paragraph (1) is approved, there shall be payable to the Controller a fee of $1,000 for each year the licence is granted.
(3) There shall be payable to the Controller on every grant of the renewal of a licence a fee of $1,000 for each year the licence is renewed.
(4) The Controller shall not refund any fee paid if the application is not approved, is withdrawn or is discontinued or if the licence is suspended or revoked.

PART III

LICENSING CRITERIA

Financial criteria, etc.
7. —(1) An applicant for a licence shall comply with the following criteria:
(a) the applicant must be a company operating in Singapore;
(b) the applicant must be insured against liability for loss of not less than $1 million for each claim arising out of any error or omission on the part of the applicant, its officers or employees;
(c) the applicant must have —
(i) not less than $2 million in paid-up capital; and
(ii) in addition, a combined paid-up capital and proof of available financing of not less than $5 million; and
(d) the applicant must obtain a performance bond or banker's guarantee in favour of the Controller in a form approved by the Controller for an amount of not less than $1 million.
(2) The performance bond or banker's guarantee referred to in paragraph (1) (*d*) may be invoked —
(a) for payment of an offer of composition made by the Controller;
(b) for payment of liabilities and rectification costs attributed to the negligence of the certification authority, its officers or employees; or

(c) for payment of the costs incurred in the discontinuation or transfer of operations of the licensed certification authority, if the certification authority's licence or operations is discontinued.

Personnel

8. —(1) An applicant shall take reasonable measures to ensure that every trusted person —
(a) is a fit and proper person to carry out the duties assigned to him;
(b) is not an undischarged bankrupt in Singapore or elsewhere or has made a composition or an arrangement with his creditors; and
(c) has not been convicted, whether in Singapore or elsewhere, of —
(i) an offence the conviction for which involved a finding that he acted fraudulently or dishonestly; or
(ii) an offence under the Act or these Regulations.
(2) Notwithstanding paragraph (1) (*c*), the Controller may allow the applicant to have a trusted person who has been convicted of an offence referred to in that paragraph, if the Controller is satisfied that —
(a) the trusted person is now a fit and proper person to carry out his duties; and
(b) 10 years have elapsed from —
(i) the date of conviction; or
(ii) the date of release from imprisonment if he was sentenced to a term of imprisonment, whichever is the later.
(3) Every trusted person must —
(a) have a good knowledge of the Act and these Regulations;
(b) be trained in the certification authority's certification practice statement; and
(c) possess the relevant technical qualifications, expertise and experience to effectively carry out his duties.

Operational criteria

9. —(1) An applicant shall comply with the following operational criteria:
(a) the applicant must have a certification practice statement approved by the Controller;
(b) the applicant must undergo and pass an initial audit before a licence can be granted by the Controller; and
(c) the applicant must undergo and pass such audit as the Controller may, by notice in writing, require.
(2) The audits referred to in this regulation must be —
(a) conducted in accordance with the auditing requirements specified in regulation 10; and
(b) completed within such time as the Controller may, by notice in writing, specify.

Auditing requirements

10. —(1) An applicant must pass any audit required under regulation 9 (1) for compliance with —
(a) security guidelines as referred to in regulation 26;
(b) licensing conditions;
(c) its certification practice statement; and
(d) the Act and these Regulations.
(2) All audits must be conducted by a qualified independent audit team approved by the Controller for this purpose comprising of a person who is a Certified Public Accountant

and a person who is a Certified Information Systems Auditor and either of whom must possess sufficient knowledge of digital signature and certificates.
(3) The firm or company to which the audit team belongs must be independent of the certification authority being audited and must not be a software or hardware vendor that is or has been providing services or supplying equipment to the certification authority.
(4) Auditing fees shall be borne by the certification authority.
(5) A copy of every audit report shall be submitted to the Controller within 4 weeks of the completion of an audit.
(6) Failure to pass the audit may be a ground for revocation of a licence.

Controller to refuse to grant or renew licences in certain circumstances
11. —(1) The Controller may refuse to grant or renew a licence if —
(a) the applicant has not provided the Controller with such information relating to it or any person employed by or associated with it for the purposes of its business, and to any circumstances likely to affect its method of conducting business, as the Controller may require;
(b) the applicant or its substantial shareholder is in the course of being wound up or liquidated;
(c) a receiver or a receiver and manager has been appointed to the applicant or its substantial shareholder;
(d) the applicant or its substantial shareholder has, whether in Singapore or elsewhere, entered into a compromise or scheme of arrangement with its creditors, being a compromise or scheme of arrangement that is still in operation;
(e) the applicant or its substantial shareholder or any trusted person has been convicted, whether in Singapore or elsewhere, of an offence the conviction for which involved a finding that it or he acted fraudulently or dishonestly, or has been convicted of an offence under the Act or these Regulations;
(f) the Controller is not satisfied as to the qualifications or experience of the trusted person who is to perform duties in connection with the holding of the licence by the applicant;
(g) the applicant fails to satisfy the Controller that it is a fit and proper person to be licensed or that all its trusted persons and substantial shareholders are fit and proper persons;
(h) the Controller has reason to believe that the applicant may not be able to act in the best interest of its subscribers, customers or participants having regard to the reputation, character, financial integrity and reliability of the applicant or any of its substantial shareholders or trusted persons;
(i) the Controller is not satisfied as to the financial standing of the applicant or its substantial shareholder;
(j) the Controller is not satisfied as to the record of past performance or expertise of the applicant or its trusted person having regard to the nature of the business which the applicant may carry on in connection with the holding of the licence;
(k) there are other circumstances which are likely to lead to the improper conduct of business by, or reflect discredit on the method of conducting the business of, the applicant or its substantial shareholder or any of the trusted persons; or
(l) the Controller is of the opinion that it is in the interest of the public to do so.
(2) For the purposes of paragraph (1), “substantial shareholder”, in relation to an applicant which is a company, has the same meaning as in the Companies Act (Cap. 50).

PART IV

REVOCATION AND SUSPENSION OF LICENCE

Revocation or suspension of licence

12. —(1) A licence shall be deemed to be revoked if the certification authority is wound up.

(2) The Controller may revoke or suspend the licence of a certification authority —

(a) on any ground on which the Controller may refuse to grant a licence under regulation 11;

(b) if the certification authority fails to comply with a direction of the Controller made under section 51 of the Act;

(c) if the certification authority is being or will be wound up;

(d) if the certification authority has entered into any composition or arrangement with its creditors;

(e) if the certification authority fails to carry on business for which it was licensed;

(f) if the Controller has reason to believe that the certification authority or its trusted person has not performed its or his duties efficiently, honestly or fairly; or

(g) if the certification authority contravenes or fails to comply with any condition or restriction applicable in respect of the licence.

(3) The Controller may revoke the licence of a certification authority at the request of that certification authority.

(4) The Controller shall not revoke the licence under paragraph (2) without first giving the certification authority an opportunity of being heard.

Powers of Controller in cases of misconduct, etc.

13. —(1) The Controller may inquire into any allegation that a certification authority, its officers or employees, is or has been guilty of any misconduct or is no longer fit to continue to remain licensed by reason of any other circumstances which have led, or are likely to lead, to the improper conduct of business by it or to reflect discredit on the method of conducting business.

(2) If, after inquiring into an allegation under paragraph (1), the Controller is of the opinion that the allegation is proved, the Controller may if he thinks fit —

(a) revoke the licence of the certification authority;

(b) suspend the licence of the certification authority for such period, or until the happening of such event, as the Controller may determine; or

(c) reprimand the certification authority.

(3) The Controller shall, at the hearing of an inquiry into an allegation under paragraph (1) against a certification authority, give the certification authority an opportunity of being heard.

(4) Where the Controller is satisfied, after making an inquiry into an allegation under paragraph (1), that the allegation has been made in bad faith or that it is otherwise frivolous or vexatious, the Controller may, by order in writing, require the person who made the allegation to pay any costs and expenses involved in the inquiry.

(5) The Controller may issue directions to the certification authority for compliance under section 51 of the Act as a result of making the inquiry.

(6) For the purposes of this regulation, “misconduct” means —

(a) any failure to comply with the requirements of the Act or these Regulations or its certification practice statement; and
(b) any act or omission relating to the conduct of business of a certification authority which is or is likely to be prejudicial to public interest.

Effect of revocation or suspension of licence
14. —(1) A certification authority whose licence is revoked or suspended under regulation 12 or 13 shall, for the purposes of this regulation, be deemed not to be licensed from the date that the Controller revokes or suspends the licence, as the case may be.
(2) A revocation or suspension of a licence of a certification authority shall not operate so as to —
(a) avoid or affect any agreement, transaction or arrangement entered into by the certification authority, whether the agreement, transaction or arrangement was entered into before or after the revocation or suspension of the licence; or
(b) affect any right, obligation or liability arising under any such agreement, transaction or arrangement.

Appeal against refusal to license, etc.
15. —(1) Where —
(a) the Controller refuses to grant or renew a licence under regulation 11;
(b) the Controller revokes a licence under regulation 12;
(c) the licence is revoked or suspended, or a certification authority is reprimanded, under regulation 13; or
(d) a performance bond or banker's guarantee is invoked under regulation 7 (2),
any person who is aggrieved by the decision of the Controller may, within 14 days after he is notified of the decision, appeal to the Minister whose decision shall be final.
(2) If an appeal is made against a decision made by the Controller, the Controller may, if he thinks fit, defer the execution of the decision, as the case may be, until a decision is made by the Minister or when the appeal is withdrawn.
(3) In considering whether to defer the execution of the decision, the Controller shall have regard to whether the deferment is prejudicial to the interests of any subscriber of the certification authority or any other party who may be adversely affected.
(4) If an appeal is made to the Minister, a copy of the appeal shall be lodged with the Controller.

PART V

CONDUCT OF BUSINESS BY LICENSED CERTIFICATION AUTHORITIES

Trustworthy record keeping and archival
16. —(1) A licensed certification authority may keep its records in the form of paper-based documents, electronic records or any other form approved by the Controller.
(2) Such records shall be indexed, stored, preserved and reproduced so as to be accurate, complete, legible and accessible to the Controller, an auditor or an authorised officer.

Trustworthy transaction logs
17. —(1) Every licensed certification authority shall make and keep in a trustworthy manner the records relating to —

(a) activities in issuance, renewal, suspension and revocation of certificates (including the process of identification of any person requesting a certificate from a licensed certification authority);
(b) the process of generating subscribers' (where applicable) or the licensed certification authority's own key pairs;
(c) the administration of a licensed certification authority's computing facilities; and
(d) such critical related activity of a licensed certification authority as may be determined by the Controller.
(2) Every licensed certification authority shall archive all certificates issued by it and maintain mechanisms to access such certificates for a period of not less than 7 years.
(3) Every licensed certification authority shall retain all records required to be kept under paragraph (1) and all logs of the creation of the archive of certificates referred to in paragraph (2) for a period of not less than 7 years.

Types of certificates
18. —(1) Subject to the approval of the Controller, a licensed certification authority may issue certificates of the following different levels of assurance:
(a) certificates which shall be considered as trustworthy certificates for the purposes of section 20 (*b*) (i) of the Act; and
(b) certificates which shall not be considered as trustworthy certificates for the purposes of section 20 (*b*) (i) of the Act.
(2) The licensed certification authority must associate a distinct certification practice statement approved by the Controller for each type of certificate issued.
(3) The licensed certification authority must draw the attention of subscribers and relying parties to the effect of using and relying on certificates that are not considered trustworthy certificates for the purposes of section 20 (*b*) (i) of the Act.

Issuance of certificates
19. —(1) In addition to the requirements specified in section 29 of the Act, every licensed certification authority shall comply with the requirements in this regulation in relation to the issuing of certificates.
(2) The certificate must contain or incorporate by reference such information as is sufficient to locate or identify one or more repositories in which notification of the revocation or suspension of the certificate will be listed if the certificate is suspended or revoked.
(3) The practices and procedures set forth in the certification practice statement of a licensed certification authority shall contain conditions with standards higher than those conditions specified in section 29 (2) of the Act.
(4) The subscriber identity verification method employed for issuance of certificates must be specified in the certification practice statement and is subject to the approval of the Controller during the application for a licence.
(5) Where a certificate is issued to a person (referred to in this regulation as the new certificate) on the basis of another valid certificate held by the same person (referred to in this regulation as the originating certificate) and subsequently the originating certificate has been suspended or revoked, the certification authority that issued the new certificate must conduct investigations to determine whether it is necessary to suspend or revoke the new certificate.

(6) The licensed certification authority must provide a reasonable opportunity for the subscriber to verify the contents of the certificate before it is accepted.
(7) If the subscriber accepts the issued certificate, the licensed certification authority shall publish a signed copy of the certificate in a repository referred to in paragraph (2).
(8) Notwithstanding paragraph (7), the licensed certification authority may contractually agree with the subscriber not to publish the certificate.
(9) If the subscriber does not accept the certificate, the licensed certification authority shall not publish it.
(10) Once the certificate has been issued by the licensed certification authority and accepted by the subscriber, the licensed certification authority shall notify the subscriber within a reasonable time of any fact known to the licensed certification authority that significantly affects the validity or reliability of the certificate.
(11) The date and time of all transactions in relation to the issuance of a certificate must be logged and kept in a trustworthy manner.

Renewal of certificates
20. —(1) Regulation 19 shall apply to the renewal of certificates as it applies to the issuance of certificates.
(2) The subscriber identity verification method shall be that specified in the certification practice statement as approved by the Controller.
(3) The date and time of all transactions in relation to the renewal of a certificate must be logged and kept in a trustworthy manner.

Suspension of certificates
21. —(1) This regulation shall apply only to every licensed certification authority which allows subscribers to request for suspension of certificates.
(2) Every licensed certification authority may provide for immediate revocation instead of suspension if the subscriber has agreed in writing.
(3) Upon receiving a request for suspension of a certificate under section 31 of the Act, the licensed certification authority shall ensure that the certificate is suspended and notice of the suspension published in the repository in accordance with section 34 of the Act.
(4) A licensed certification authority may suspend a certificate that it has issued if the licensed certification authority has reasonable grounds to believe that the certificate is unreliable, regardless of whether the subscriber consents to the suspension; but the licensed certification authority shall complete its investigation into the reliability of the certificate and decide within a reasonable time whether to reinstate the certificate or to revoke the certificate in accordance with section 32 or 33 of the Act.
(5) It is the responsibility of any person relying on a certificate to check whether a certificate has been suspended.
(6) A licensed certification authority shall suspend a certificate after receiving a valid request for suspension (in accordance with section 31 of the Act); but if the licensed certification authority considers that revocation is justified in the light of all the evidence available to it, the certificate must be revoked in accordance with section 32 or 33 of the Act.
(7) A licensed certification authority shall check with the subscriber or his authorised agent whether the certificate should be revoked and whether to reinstate the certificate after suspension.

(8) A licensed certification authority must terminate a suspension initiated by request if the licensed certification authority discovers and confirms that the request for suspension was made without authorisation by the subscriber or his authorised agent.
(9) If the suspension of a certificate leads to a revocation of the certificate, the requirements for revocation shall apply.
(10) The date and time of all transactions in relation to the suspension of certificates must be logged and kept in a trustworthy manner.
(11) A licensed certification authority must maintain facilities to receive and act upon requests for suspension at all times of the day and on all days of every year.

Revocation of certificates
22. —(1) In order to confirm the identity of the subscriber or authorised agent making a request for revocation under section 32 (*a*) of the Act, the licensed certification authority must use the subscriber identity verification method specified in the certification practice statement for this purpose.
(2) A licensed certification authority must, after receiving a request for revocation, verify the request, revoke the certificate and publish notification of it under section 35 of the Act.
(3) A licensed certification authority must maintain facilities to receive and act upon requests for revocation at all times of the day and on all days of every year.
(4) A licensed certification authority shall give notice to the subscriber immediately upon the revocation of a certificate.
(5) The date and time of all transactions in relation to the revocation of certificates must be logged and kept in a trustworthy manner.

Expiry date of certificates
23. A certificate must state the date on which it expires.

Certification practice statement
24. —(1) Every licensed certification authority shall use the Internet draft of the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, adopted by the Internet Engineering Task Force and reproduced by the Controller on its Internet website, as a guide for the preparation of its certification practice statement.
(2) Any change to the certification practice statement during the term of the licence requires the prior approval of the Controller.
(3) Every licensed certification authority must highlight to its subscribers any limitation of their liabilities and, in particular, it must draw the subscribers' attention to the implication of reliance limits on their certificates.
(4) The subscriber identity verification method for the issuance, suspension, revocation and renewal of a certificate must be specified in the certification practice statement.
(5) A copy of the latest version of the certification practice statement, together with its effective date, must be filed with the Controller and published on the certification authority's Internet website accessible to members of the public.
(6) After the effective date, the latest version filed with the Controller will be the prevailing version for a particular certificate.
(7) Every licensed certification authority must log all changes to the certification practice statement together with the effective date of each change.

(8) A licensed certification authority shall keep in a trustworthy manner a copy of each version of the certification practice statement, together with the date it came into effect and the date it ceased to have effect.

Secure digital signatures

25. —(1) The technical implementation of the requirements in section 20 of the Act shall be such as to ensure that it is computationally infeasible for any person other than the person to whom the signature correlates to have created a digital signature which is verified by reference to the public key listed in that person's certificate.

(2) The signature on its own should be such as to —

(a) ensure that the name or other unique identifiable notation of the person to whom the signature correlates be incorporated as part of the signature and cannot be replaced or forged; and

(b) readily present such indicia of identity to a person intending to rely on the signature.

(3) The technical implementation should ensure that —

(a) the steps taken towards the creation of the signature must be under the direction of the person to whom the signature correlates; and

(b) no other person can reproduce the sequence of steps to create the signature and thereby create a valid signature without the involvement or the knowledge of the person to whom the signature correlates.

(4) The technical implementation should indicate to a relying party of a signature whether the document or record that the signature purports to sign has been modified in anyway and this indication should be revealed in the process of verifying the signature.

Security guidelines

26. —(1) Every licensed certification authority shall ensure that in the performance of its services it materially satisfies the security guidelines determined by the Controller and published on the Controller’s Internet website.

(2) An auditor when determining whether a departure from the security guidelines is material shall exercise reasonable professional judgment as to whether a condition that does not strictly comply with the guidelines is or is not material, taking into consideration the circumstances and the system as a whole.

(3) Without prejudice to the generality of situations which the auditor may consider to be material, the following incidents of non-compliance shall be considered to be material:

(a) any non-compliance relating to the validity of a certificate;

(b) the performance of the functions of a trusted person by a person who is not suitably qualified; or

(c) the use by a licensed certification authority of any system other than a trustworthy system.

(4) The security guidelines shall be interpreted in a manner that is reasonable in relation to the context in which a system is used and is consistent with other laws.

(5) Notwithstanding an auditor's assessment of whether a departure from the security guidelines is material, the Controller may make his own assessment and reach a conclusion for the purpose of paragraph (1) which is at variance with that of the auditor.

(6) Every licensed certification authority shall provide every subscriber with a trustworthy system to generate his key pair.

(7) Every licensed certification authority shall provide the mechanism to generate and verify digital signatures in a trustworthy manner and the mechanism provided shall also indicate the validity of the signature.
(8) If the digital signature is not valid, the mechanism provided should indicate if the invalidity is due to the integrity of the document or the signature and the mechanism provided shall also indicate the status of the certificate.
(9) For mechanisms provided by third parties other than the licensed certification authority, the resulting signature is considered secure only if the licensed certification authority endorses the implementation of such mechanisms in conjunction with its certificate.
(10) Every licensed certification authority shall be responsible for the storage of keys (including the subscriber's key and the licensed certification authority's own key) in a trustworthy manner.
(11) The Controller may, from time to time, publish on its Internet website further details of the security guidelines for compliance by every licensed certification authority.

Incident handling
27. —(1) A licensed certification authority shall implement an incident management plan that must provide at the least for management of the following incidents:
(a) compromise of key;
(b) penetration of CA system and network;
(c) unavailability of infrastructure; and
(d) fraudulent registration and generation of certificates, certificate suspension and revocation information.
(2) If any incident referred to in paragraph (1) occurs, it shall be reported to the Controller within 24 hours.

Confidentiality
28. —(1) Except for the purposes of Part XII of the Act, or for any prosecution under any written law or pursuant to an order of court, every licensed certification authority and its authorised agent must keep all subscriber-specific information confidential.
(2) Any disclosure of subscriber-specific information by the licensed certification authority or its agent must be authorised by the subscriber.
(3) This regulation shall not apply to subscriber-specific information which —
(a) is contained in the certificate for public disclosure;
(b) is otherwise provided by the subscriber to the licensed certification authority for this purpose; or
(c) relates to the fact that the certificate has been revoked or suspended.

Change in management
29. A licensed certification authority shall inform the Controller of any changes in the appointment of any person as its director or chief executive, or of any person to perform functions equivalent to that of a chief executive, within 3 working days from the date of appointment of that person.

PART VI

REQUIREMENTS FOR REPOSITORY

Availability of general purpose repository

30. —(1) A general purpose repository shall be available at all times of the day and on all days of every year.

(2) A general purpose repository must ensure that the total aggregate period of any down time in any period of one month shall not exceed 0.3% of the period.

(3) Any down time, whether scheduled or unscheduled, shall not exceed 30 minutes duration at any one time.

Specific purpose repository

31. Subject to the approval of the Controller, a repository may be dedicated for a specific purpose for which specific hours of operation may be acceptable.

PART VII

APPLICATION TO GOVERNMENT AND STATUTORY CORPORATIONS

Application to Government and statutory corporations

32. —(1) For the purposes of section 20 (*b*) (iii) of the Act, a department or ministry of the Government, an organ of State or a statutory corporation that is approved by the Minister under that section to act as a certification authority shall comply with the provisions of Parts III (with the exception of regulations 7 and 11), IV (with the exception of regulations 12, 14 and 15), V (with the exception of regulation 29), VI, VII and VIII (with the exception of regulations 36 and 37) as if it were a licensed certification authority.

(2) The provisions referred to in paragraph (1) shall apply, with the necessary modifications and such other modifications as the Controller may determine, to the department or ministry of the Government, an organ of State or a statutory corporation that is approved by the Minister under section 20 (*b*) (iii) of the Act.

PART VIII

ADMINISTRATION

Waiver

33. —(1) Any licensed certification authority that wishes to apply for a waiver of any of the requirements specified in these Regulations may apply in writing to the Controller at the time when it submits an application for a licence.

(2) The application must be supported by reasons for the application and include the necessary supporting documents.

Disclosure

34. —(1) The licensed certification authority must submit half-yearly progress and financial reports to the Controller.

(2) The half-yearly progress reports must include information on —

(a) the number of subscribers;

(b) the number of certificates issued, suspended, revoked, expired and renewed;

(c) system performance including system up and down time and any extraordinary incidents;
(d) changes in the organisational structure of the certification authority;
(e) changes since the preceding progress report submitted or since the application for the licence; and
(f) changes in the particulars of any trusted person since the last submission to the Controller, including the name, identification number, residential address, designation, function and date of employment of the trusted person.
(3) The licensed certification authority has a continuing obligation to disclose to the Controller any changes in the information submitted.
(4) All current versions of the licensed certification authority's applicable certification practice statements together with their effective dates must be published in the licensed certification authority's Internet website.

Discontinuation of operations of licensed certification authority
35. —(1) If a licensed certification authority intends to discontinue its operations, the licensed certification authority may arrange for its subscribers to re-subscribe to another licensed certification authority.
(2) The licensed certification authority shall make arrangements for its records and certificates to be archived in a trustworthy manner.
(3) If the records are transferred to another licensed certification authority, the transfer must be done in a trustworthy manner.
(4) A licensed certification authority shall —
(a) give the Controller a minimum of 3 months' written notice of its intention to discontinue its operations;
(b) give its subscribers a minimum of 2 months' written notice of its intention to discontinue its operations; and
(c) advertise, in such daily newspaper and in such manner as the Controller may determine, at least 2 months' notice of its intention to discontinue its operations.

Penalties
36. Any person who fails, without any reasonable excuse, to comply with regulation 16 (2), 17, 19 (2) or (11), 20 (3), 21 (10), 22 (5), 24 (7) or (8) or 28 shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 and, in the case of a second or subsequent conviction, to a fine not exceeding $10,000.

Composition of offences
37. Any offence under these Regulations may be compounded by the Controller under section 59 of the Act.

[G.N. No.S 60/99]

ANNEX B

PROPOSED LEGISLATIVE AMENDMENTS RELATING TO ELECTRONIC GOVERNMENT

The proposed amendments set out below are intended for the purposes of discussion. Changes to the existing provisions are indicated in *italics*.

A. Proposed new definition in section 2

"Government agency" means a department or ministry of the Government, an organ of state or a statutory body;

Notes

Definition of terms

A.1 The term "**Government agency**" replaces the words "a department or ministry of the Government, organ of State or statutory corporation" in the ETA. The term statutory "body" has been substituted for wider application since some entities created by statute to carry out government or regulatory functions are not corporations e.g. the Medical Council.

B. Proposed amendments to section 9

Retention of electronic records **9.** —(1) Where a rule of law requires that certain documents, records or information be retained, *or provides for certain consequences if it is not,* that requirement is satisfied by retaining them in the form of electronic records if the following conditions are satisfied: (a) the information contained therein remains accessible so as to be usable for subsequent reference; (b) the electronic record is retained in the format in which it was originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received; (c) such information, if any, as enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received, is retained; *and*

(d) any additional requirements relating to the retention of electronic records specified by the Government agency which has supervision over the requirement for retention of such records are complied with.
(2) An obligation to retain documents, records or information in accordance with subsection (1) (*c*) shall not extend to any information necessarily and automatically generated solely for the purpose of enabling a record to be sent or received.
(3) A person may satisfy the requirement referred to in subsection (1) by using the services of any other person, if the conditions in paragraphs (*a*) to (*d*) of that subsection are complied with.
(4) Nothing in this section shall apply to —
(a) any rule of law which expressly provides for the retention of documents, records or information in the form of electronic records; or
(b) any rule of law requiring that any documents, records or information be retained if the Minister has, by order in the Gazette, specified that this section shall not apply to that requirement in respect of those documents.

B.1 The words "or provides for certain consequences if it is not" are added in section 9(1) for consistency with the other provisions in Part II of the ETA e.g. sections 7 and 8. This is because a legal requirement may not make the retention of documents mandatory, but merely provide that if the documents are not retained, the person will suffer some consequences or handicap.

B.2 New section 9(1)(*d*) allows Government agencies to impose additional requirements on the retention of documents under their purview. It is based on existing section 9(4)(*b*) (replaced by the opt-out provision discussed in B.3).

B.3 New section 9(4)(*b*) allows Government agencies to opt out of section 9 by specifying accordingly in an order published in the *Gazette*.

C. Proposed new section 9A

Provision of originals
9A. *— (1) Where a rule of law requires any document, record or information to be provided or retained in its original form, or provides for certain consequences if it is not, that requirement is satisfied by providing or retaining the document, record or information in the form of an electronic record if the following conditions are satisfied:*

(a) there exists a reliable assurance as to the integrity of the information contained in the electronic record from the time the document, record or information was first made in its final form, whether as a document in writing or as an electronic record;
(b) where the document, record or information is to be provided to a person in its original form, the electronic record that is provided to the person is accessible by the person and capable of being retained by the person so as to be usable for subsequent reference; and
(c) any additional requirements relating to the provision or retention of such electronic records specified by the Government agency which has supervision over the requirement for the provision or retention of such records are complied with.
(2) For the purposes of subsection (1)(a) —
(a) the criterion for assessing integrity shall be whether the information has remained complete and unaltered, apart from the introduction of any changes that arise in the normal course of communication, storage and display; and
(b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the circumstances.
(3) A person may satisfy the requirement referred to in subsection (1) by using the services of any other person, if the conditions in paragraphs (a) to (c) of that subsection are complied with.
(4) Nothing in this section shall apply to any rule of law requiring that any documents, records or information be provided or retained in original form if the Minister has, by order in the Gazette, specified that this section shall not apply to that requirement in respect of those documents.

Notes

C.1 This provision is based on article 8 of the UNCITRAL Model Law. It however adopts the test of accessibility adopted in various other jurisdictions, instead of the "capable of display" test in article 8 of the UNCITRAL Model Law.

C.2 The words "or provides for certain consequences if it is not" are included for consistency with the other provisions in Part II of the ETA e.g. sections 7, 8 and 9 (as amended). This is because a legal requirement may not make the production or retention of originals mandatory, but merely provide that if the documents are not produced or retained, the person will suffer some consequences or handicap.

C.2 Section 9A(1)(*c*) allows Government agencies to impose additional requirements on the retention of documents under their purview. It mirrors proposed section 9(1)(*d*) above.

C.3 Section 9A(4) allows Government agencies to opt out of section 9A by specifying accordingly in an order published in the *Gazette*. It mirrors proposed section 9(4)(*b*) above.

D. Proposed amendments to section 47

Acceptance of electronic filing and issue of documents

47 —(1) Any *Government agency* that, pursuant to any written law —

(*a*) accepts the filing of documents, *obtains information in any form*;

(*b*) requires that documents be created or retained;

(*c*) *requires documents, records or information to be produced or retained in their original form;*

(*d*) issues any permit, licence or approval; or

(*e*) provides for the method and manner of payment,

may, notwithstanding anything to the contrary in such written law, *carry out that function by means of electronic records or in electronic form.*

(2) In any case where a *Government agency* decides to perform any of the functions referred to in subsection (1) *by means of electronic records or in electronic form, the Government* agency may specify —

(*a*) the manner and format in which such electronic records shall be filed, created, retained, issued *or produced*;

(*b*) where such electronic records have to be signed, the type of electronic signature required (including, if applicable, a requirement that the sender use a digital signature or other secure electronic signature);

(*c*) the manner and format in which such signature shall be affixed to the electronic record, and the identity of or criteria that shall be met by any certification authority used by the person filing the document;

(*d*) control processes and procedures as appropriate to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(*e*) any other required attributes for electronic records or payments that are currently specified for corresponding paper documents.

(3) For the avoidance of doubt, notwithstanding anything to the contrary in any written law but subject to any specification made under subsection (2), where any person is required by any written law to —

(a) file any document with or provide information in any form to a Government agency;

(b) create or retain any document for a Government agency;

(c) use a prescribed form for an application or notification to, or other transaction with, a Government agency;

(d) produce to or retain for a Government agency any document, record or information in its original form; or

(e) hold a licence, permit or other approval from a Government agency,

such a requirement is satisfied by an electronic record specified by the Government agency for that purpose and —

(i) in the case of a requirement referred to in paragraph (a), (c) or (d), transmitted or retained (as the case may be) in the manner specified by the Government agency;

(ii) in the case of a requirement referred to in paragraph (b), respectively created or retained in the manner specified by the Government agency; or

(iii) in the case of a requirement referred to in paragraph (e), issued by the Government agency.

(*4*) *Subject to sections 9 and 9A,* nothing in this Act shall by itself compel any *Government agency* to accept or issue any document *or information* in the form of electronic records or to accept any payment in electronic form.

Notes

D.1 The words "any department or ministry of the Government, organ of State or statutory corporation" in section 47 are replaced by the term "Government agency" for simplicity. The term "Government agency" will be defined accordingly in section 2 of the ETA (See A in this Annex).

D.2 **Section 47(1)** - This subsection empowers Government agencies to adopt electronic means of carrying out their functions under written law. The amendments expand on the functions currently covered by the provision.

D.3 Currently, section 47(1)(*a*) applies only to the filing, creation and retention of *documents*. The inclusion of a reference to the obtaining of information in any form will extend the provision to situations where a document is not

required, for example, a requirement to orally inform the Government agency. This issue is discussed in Part 4.8.

D.4 New section 47(1)(*c*) extends the provision to the requirement for production of original documents. New subsections (1)(*c*) and (3)(*d*) make it clear that electronic copies of paper originals or electronic originals can satisfy any requirement under written law for production of paper originals. This issue is discussed in Part 4.11.

D.5 **Section 47(2)** - This largely reproduces the existing subsection (2) which empowers the Government agency to specify certain matters where it decides to perform the functions referred to in subsection (1) electronically.

D.6 **Section 47(3)** - This new subsection makes it clear that certain functions carried out by a Government agency electronically satisfy the relevant requirements under written law. The functions covered by subsection (3) generally reflect the functions referred to in subsection (1).

D.7 Section 47(3)(*c*) specifically refers to the requirement for prescribed forms. New section 47(3) validates the use of such forms whether or not they resemble the prescribed paper forms. This issue is discussed in Part 4.7.

ANNEX C

Comment on the draft UNCITRAL Convention on the Use of Electronic Communications in International Contracts (submitted to UNCITRAL Secretariat on 16 May 2005)

1 Singapore expresses its appreciation to Working Group IV on the completion of its work at the forty-fourth session, and considers that the revised version of the draft convention A/CN.9/577 represents a sound basis for consideration and adoption by the Commission.

2 At this juncture, we wish to highlight only certain limited issues which we feel were not fully considered by the Working Group IV in its deliberations. We propose that the Commission consider:

(a) amending paragraph 3(a) of article 9 of the draft Convention (A/CN.9/577) to recognise that electronic signatures are sometimes required by law only for the purpose of identifying the person signing ("the signor") and associating the information with the signor, but not necessarily to indicate the signor's "approval" of the information contained in the electronic communication; and

(b) deleting paragraph 3(b) of article 9 of the draft Convention (A/CN.9/577), to achieve functional equivalence between handwritten signatures and electronic signatures, and to avoid the unintended difficulties that would be created by the inclusion of the general legal "reliability requirement" in paragraph 3(b).

Issues relating to paragraph 3(a) of article 9

3 Paragraph 3(a) of article 9 lays down general criteria for functional equivalence between handwritten signatures and electronic signatures.[348] Paragraph 3(a) provides that only an electronic signature that fulfils both the function of identification of the party *as well as* the function of indicating that party's approval of the information contained in the electronic communication meets that legal requirement of a signature in relation to an electronic communication.[349]

---

[348] Paragraph 3(a) of Article 9 is based on Article 7, paragraph 1(a) of the UNICTRAL Model Law on Electronic Commerce 1996. Article 7 of the UNCITRAL Model Law on Electronic Commerce states:

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

[349] It should be noted that under paragraph 3 of article 9, which originated from article 7, paragraph 1 of the UNCITRAL Model Law on Electronic Commerce, the mere signing of an electronic communication by means of a functional equivalent of a handwritten signature is not intended, in and of itself, to confer legal validity on the data message. Whether an electronic communication that fulfilled the requirement of a signature has legal validity is to be settled under

4 However, there may be instances where the law requires a signature that does not fulfil the function of indicating the signing party's approval of the information contained in the electronic communication. For example, many countries have requirements of law for notarisation of a document by a notary or attestation by a commissioner for oath. In such cases, it is not the intention of the law to require the notary or commissioner, by signing, to indicate his approval of the information contained in the electronic communication. In such cases, the signature of the notary or commissioner merely identifies the notary or commissioner, and associates the notary or commissioner with the contents of the document, but does not indicate the approval by the notary or commissioner of the information contained in the document. Similarly, there may be laws that require the execution of a document to be witnessed by a witness, who may be required to append his signature to that document. The signature of the witness merely identifies the witness and associates the witness with the contents of the document witnessed, but does not indicate the approval by the witness of the information contained in the document.

5 The conjunctive requirement in paragraph 3(a) of article 9 would prevent electronic signatures from satisfying the requirement of law for a signature in such situations where the function of indicating approval of the contents of the electronic communication cannot be fulfilled by such signatures.

6 In order to also allow electronic signatures that are not intended to fulfil the function of indicating the signor's approval of the information contained in the electronic communication, to also satisfy a requirement of law for a signature, we therefore propose that paragraph 3(a) of article 9 should be amended to read as follows:

> "(a) A method is used to identify the party and to associate that party with the information contained in the electronic communication, and as may be appropriate in relation to that legal requirement, to indicate that the party's approval of the information contained in the electronic communication; and".

7 The phrase "*A method is used to identify the party and to associate that party with the information contained in the electronic communication*" represents the minimum functional requirements of any signature, handwritten or electronic. This phrase provides that electronic signatures that only fulfil these minimum functions will satisfy the requirement of law for signatures. The phrase "*and as may be appropriate in relation to that legal requirement*" recognises that the function that the electronic signature is intended to perform will depend on the policy or purpose behind that particular requirement of law in question, and provides that the electronic signature is required to fulfil the function of indicating the signing party's approval of the information contained in the electronic communication, where it is appropriate in relation to that legal requirement. For example, if the law requires a party to sign an offer document to indicate his acceptance of the terms contained in the document, that electronic signature would fulfil the requirements of the proposed paragraph 3(a) of article 9 if it identifies the signing party, associates that party with the information contained in the document **and** indicates that party's approval of the information contained in the document.

---

the law applicable outside the draft convention. See paragraph 61 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996).

Issues relating to paragraph 3(b) of article 9

8 Paragraph 3(b) of article 9 contains a requirement that the method of signing must be "as reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement" in order for the electronic signature to be legally valid.

9 This "reliability requirement" in paragraph 3(b) of article 9 has its origins in article 7, paragraph 1(b) of the UNCITRAL Model Law on Electronic Commerce 1996.

10 In the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures 2001, it was already noted that article 7 of the UNCITRAL Model Law on Electronic Commerce creates uncertainty as the determination of appropriately sufficient reliability can only be made *ex post* by a court or other trier of fact. In order to create more certainty *ex ante*, Article 6, paragraph 3 of the UNCITRAL Model Law on Electronic Signatures 2001 was introduced. Paragraph 118 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures 2001 states:

> … However, under article 7 of the UNCITRAL Model Law on Electronic Commerce, the determination of what constitutes a reliable method of signature in the light of the circumstances, can be made only by a court or other trier of fact intervening *ex post*, possibly long after the electronic signature has been used. In contrast, the new Model Law [on Electronic Signatures 2001] is expected to create a benefit in favour of certain techniques, which are recognised as particularly reliable, irrespective of the circumstances in which they are used. That is the purpose of paragraph 3, which is expected to create certainty (through either a presumption or a substantive rule), at or before the time any such technique of electronic signature is used (*ex ante*), that using a recognised technique will result in legal effects equivalent to those of a handwritten signature. Thus, paragraph 3 is an essential provision if the new Model Law is to meet its goal of *providing more certainty than readily offered by the UNCITRAL Model Law on Electronic Commerce* as to the legal effect to be expected from the use of particularly reliable types of electronic signatures. …" [Emphasis added]

11 At the forty-second session, the Working Group had considered two variants in paragraph 3 of article 9. Variant A was based on article 7 of the UNCITRAL Model Law on Electronic Commerce, while variant B was based on article 6, paragraph 3 of the UNCITRAL Model Law on Electronic Signatures.[350] The Working Group decided in favour of retaining variant A only.[351]

12 In choosing to retain only variant A, the Working Group may not have fully considered the implications of retaining in paragraph 3(b) of article 9, the general "reliability requirement" based on article 7 of the Model Law on Electronic Commerce.

[350] A/CN.9/546, paragraph 48.
[351] A/CN.9/546, paragraph 54-57.

13 Under paragraph 3(b) of article 9, the satisfaction by an electronic signature of a requirement of law for signature depends on whether the signature method was appropriately reliable for the purpose of the electronic communication in light of all the circumstances, as determined *ex post* by a court or other trier of fact. This means that the parties to the electronic communication or contract are not able to know with certainty *ex ante* whether the electronic signature used will be upheld by a court or other trier of fact as "appropriately reliable" and therefore not be denied legal validity, until after a legal dispute arises subsequently. It also means that even if there was *no dispute* about the identity of the person signing or the fact of signing (i.e. no dispute as to authenticity of the electronic signature), a court or trier of fact may still rule that the electronic signature was not appropriately reliable, and therefore invalidate the entire contract.

14 Such a provision will potentially have serious practical implications for electronic commerce:

(a) It will create uncertainty in electronic transactions because whether a signature method is appropriately reliable and hence not be denied legal validity will be determined *ex post* by the court or trier of fact, and not *ex ante* by the parties. Although parties can exercise party autonomy by agreeing on a signature method, it remains that the parties' agreement is only one of the factors in paragraph 3(b) of article 9 taken into consideration by the court or trier of fact.[352] Even if the parties were satisfied at the outset as to the reliability of the signature method, a court or trier of fact may rule otherwise.

(b) It could be used to the detriment of the very class of persons that the legal requirements for signature are intended to protect. A party could try to invalidate his own electronic signature as being insufficiently reliable, in order to invalidate a contract, where it is convenient to him. This would be to the detriment of the other party relying on the signor's signature. This provision then risks becoming a trap for the unwary or a loophole for the unscrupulous.

(c) It may be an impediment to electronic commerce. It will add to business costs if users feel compelled to use more sophisticated and costly technology to ensure that the reliability requirement is satisfied. Conversely, such uncertainty and additional costs may even discourage the use of electronic transactions.

15 It is noted that the reliability requirement originated from language in laws relating to the closed and heavily regulated area of funds transfer.[353] In that context, the question of

[352] This was explicitly noted at paragraph 60 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996), which states, "However, a possible agreement between originators and addressees of data messages as to the use of a method of authentication is not conclusive evidence of whether that method is reliable or not."

[353] See A/CN.9/387, paragraphs 81 to 87. At the 26th session of the Working Group on Electronic Data Interchange, which considered the Draft Provisions for Uniform Rules on the Legal Aspects of Electronic Data Interchange (EDI) and Related Means of Trade Data Communication (which later revisions became the Model Law on Electronic Commerce), an earlier draft of article 7 contained the phrase "and the mode of identification of the sender is in the circumstances a **[commercially] reasonable** method of security against unauthorized messages", before it was suggested that the phrase be replaced by "a method of authentication is

whether the authentication or security procedure, e.g. a signature, is appropriate relates to the concept of attribution of that signature to the person. The UNCITRAL Model Law on Electronic Commerce originally needed a reliability test because it contained a general attribution rule in article 13.[354] In the Model Law on Electronic Commerce, article 7 and article 13 together affirmed the validity of an electronic signature and allowed the attribution of the data message to an originator as long as the addressee used a method agreed upon with the originator to verify the authenticity of the message, without the need to demonstrate the authenticity of the signature itself.[355] The attribution rule in the UNCITRAL Model Law on Electronic Commerce was ultimately limited to technology agreed between the signor and the relying party.

16 The draft convention does not deal with the attribution of electronic communications.[356] Therefore, the current paragraph 3(b) of article 9 of the draft convention imposes a general "reliability requirement" without any corollary attribution provision. In the absence of an acceptable attribution rule, attribution of a signature should be a matter of proof. There is no necessity for a "reliability requirement" to be introduced as a complement to a non-existent attribution rule.

17 It is noted that there is no such "reliability requirement" for the legal validity of handwritten signatures (or any of the other marks on paper that may constitute a signature at law). Common law does not impose any form requirement on signatures. A person can sign by marking a cross "X" on a document. A person can also sign by a machine that prints his name on a document. Both the cross "X" and machine-printed name are legally valid signatures, though questions of proof may arise. In each case, it is a matter of proof whether the purported signor did in fact sign in that manner and intended thereby to sign the document. In order to establish the signature's function of linking the signor with the signed document, the context of the signing will always have to be demonstrated, whether the signature is on paper or electronic.

18 It is not the form of the signature, but the proven link between the signature and the purported signor based on the context, that gives the signature its legal effect. In our view, electronic signatures are merely another form of signature, and should in principle be legally valid as signatures without any special requirements of reliability. Questions of proof of the making of the signature (which exist for both handwritten and electronic signatures) should not distort the law on the validity of signatures. If it is recognised that the legal effect of a signature is based on the proven link between the document, the signature and the purported signor, then it is irrelevant whether the signature method was of an appropriate level of reliability. In order to achieve functional equivalence between handwritten signatures and electronic signatures, there should not be any additional

---

sufficient if it is **as reliable as is appropriate** in all the circumstances to the purpose for which a communication was made". The phrase "commercially reasonable" originated from language used in article 5 of the UNCITRAL Model Law on International Credit Transfers, and Article 4A of the Uniform Commercial Code (UCC).

[354] If, as a matter of law, a signature is to be attributed to a particular person, then in fairness to that person it is necessary to ensure that the technical features of the signature are technically reliable.

[355] A/CN.9/571, paragraph 127.

[356] A/CN.9/546, paragraph 127.

reliability requirement for electronic signatures as contained in paragraph 3(b) of article 9.

19 In commercial transactions, the person relying on a signature always takes the risk that the signature is not genuine, so he evaluates the risk that the signature is not genuine and protects himself accordingly.[357] The risk analysis will of course include the cost of having the signature made more reliable and the cost of its being not genuine. So a history of dealings with the purported signor, or a low-value transaction, may persuade someone to rely on a signature that would not be satisfactory if it were from a stranger or for a high value transaction. These precautions and judgments are not a matter of law but a matter of prudence. That is, a party may not feel comfortable about relying on a signature in the form of a cross "X", but that is a judgment by that party as a matter of prudence, and not a matter of law, as the signature in the form of a cross "X" is fully valid as a signature at law. We are of the view that this analysis applies equally where electronic commercial transactions and electronic signatures are concerned.

20 We recognise that people have had many years of experience in evaluating how reliable a handwritten signature is, and therefore are able to easily judge what types of handwritten signatures are prudent to be relied upon. People are currently less familiar with the potentials and vulnerabilities of methods of signing electronically, and may be less proficient in making that prudential judgment. However, the law does not add any value to this lack of familiarity by introducing a general reliability requirement such as paragraph 3(b) of article 9. Such a reliability requirement merely transfers the prudential judgment from the relying party to the judge or adjudicator. The judge or adjudicator may be no more competent to make that prudential judgment, although he or she may have the benefit of expert evidence. Such expert evidence is also available to the relying party, but at a more useful point of time, before the transaction is consummated. As people become more familiar with electronic signatures, they will become more experienced at making that prudential judgment.

21 We note that in order to achieve the objective of harmonisation of laws relating to electronic commerce, the draft convention should contain either a uniform standard for the reliability requirement for electronic signatures (which can be in the form of a general "reliability requirement" as in paragraph 3(b) of article 9), or no reliability requirement (which will be achieved if paragraph 3(b) of article 9 were deleted). As pointed out above, the current paragraph 3(b) of article 9 creates significant uncertainty which does not promote the use of electronic commerce, and we are of the view that such a reliability requirement is unnecessary and inappropriate in the circumstances. We therefore propose that the better and more appropriate option is to have no reliability requirement for electronic signatures, and that paragraph 3(b) of article 9 be deleted.

22 If paragraph 3(b) of article 9 (and therefore the reliability requirement) is deleted, article 9 will provide that *all electronic signatures* that fulfil the functions described in paragraph 3(a) of article 9 will satisfy the requirement of law for signatures. This will

[357] This may involve checking the signature against known genuine versions of it, or getting the signature witnessed, notarized or guaranteed by a bank, etc.

provide parties with the certainty of knowing that the electronic signatures appended by them or being relied upon by them do satisfy the requirement of law for signatures, and therefore would not be denied legal validity on that basis.

ANNEX D

LEGISLATION REFERENCES

Singapore
Electronic Transactions Act (Cap.88) (1998)
Singapore Statutes online, available via *http://www.ecitizen.gov.s,* under Useful Links.

Australia
http://www.austlii.org/
Commonwealth Electronic Transactions Act 2000
New South Wales Electronic Transactions Act 2000
http://www.legislation.nsw.gov.au/
Electronic Transactions (Victoria) Act 2000
http://www.dms.dpc.vic.gov.au/

Canada
Uniform Electronic Commerce Act
http://www.ulcc.ca/
British Columbia Electronic Transactions Act (2001)
http://www.bcsolutions.gov.bc.ca/qp/
New Brunswick Electronic Transactions Act (2001)
http://www.gnb.cal
Ontario Electronic Commerce Act 2000
Manitoba Electronic Commerce and Information Act 2000

Hong Kong
Electronic Transactions Ordinance (Cap.553)
http://www.legislation.gov.hk/index.htm

Ireland
Electronic Commerce Act 2000
http://irlgov.ie/bills28/acts/2000/default.htm

New Zealand
Electronic Transactions Act 2002
http://www.legislation.govt.nz/

UK
Electronic Communications Act 2000
Electronic Commerce (EC Directive) Regulations 2002
http://www.opsi.gov.uk/

US
Electronic Signatures in Global and National Commerce Act (E-SIGN Act) (2000)
http://www.access.gpo.gov/

UNCITRAL
http://www.uncitral.org/
Model Law on Electronic Signatures (2001)
Model Law on Electronic Commerce, with Guide to Enactment (1996) and article 6*bis* (1998)
Draft Convention on Electronic Contracting draft before the 38th session of UNCITRAL (Vienna, 4-15 July 2005), see A/CN.9/577

EU
http://europa.eu.int/
Directive on Electronic Signatures (Directive 1999/93/EC)
Directive on Electronic Commerce (Directive 2000/31/EC)

The Commonwealth Secretariat
Model Law on Electronic Transactions
http://www.thecommonwealth.org

ANNEX E

LIST OF QUESTIONS

Q1. Do you have any comments on the proposal to move technology specific details in the ETA to the ETR?

Q2. Do you have any comments on the proposal to replace the current "licensing" approach to an "accreditation" approach in the ETA and ETR? (See Annex A)

Q3. Do you have any comments on the proposed amendments to the financial criteria and fees for CA accreditation?

Q4. Do you have any comments on the proposed increase in the accreditation duration from 1 year to 2 years?

Q5. Do you have any comments on the proposed amendments to limit the audit requirement to relevant security guidelines?

Q6. Is it necessary to clarify the meaning of "network service provider". Do you agree with the proposed definition of "network service provider"? (See definition proposed for discussion in paragraph 3.4.8)

Q7. Do you agree with the proposed deletion of the words "to which he merely provides access" in section 10(1) of the ETA? (See paragraph 3.4.14)

Q8. If section 10 of the ETA is amended as proposed in paragraphs 3.4.8 and 3.4.14, do you think any further safeguards are necessary? In particular, would the protection given under section 10 be too wide? (See paragraph 3.4.22). If yes, please elaborate with reference to specific kinds of liability from which network service providers should not be exempted.

Q9. Should the immunity regime for service providers under section 10 of the ETA be changed (other than the changes mentioned in Q.6, 7 and 8)?

Q10. Do you have any comments on the proposed amendments to section 9 of the ETA in Annex B?

Q11. Do you have any comments on the proposed amendments to section 47 of the ETA in Annex B?

Q12. Should Singapore adopt a single provision on electronic originals or provide specifically for different situations in which electronic communications may be used as a functional equivalent of paper or other non-electronic forms?[358] (See paragraphs 4.12.1 to 4.12.9, especially paragraphs 4.12.8 and 4.12.9).

Q13. Should consent to accept electronic originals be required? In this respect, should there be any distinction between Government agencies and private persons or entities, and if yes, what differences should there be? For example, should Government agencies be presumed to accept electronic originals unless they have opted out of doing so, as proposed in section 9A(4) in Annex B? Would your views differ if, instead of a single provision on electronic originals, there are specific provisions on the use of electronic communications in different situations? (See paragraphs 4.12.10 to 4.12.12).

Q14. Proposed sections 9 and 9A of the ETA[359] require compliance with any additional technical requirements as to form and procedure that Government agencies may have in relation to the acceptance of electronic originals. Should there be express requirements to comply with such additional technical requirements in the case where the intended recipient of electronic originals is not a Government agency? Would your views differ if, instead of a single provision on electronic originals, there are specific provisions on the use of electronic communications in different situations? (See paragraphs 4.12.13 to 4.12.16)

Q15. Do you agree that the definition of an electronic signature should not require such a signature to fulfill both an identification as well as an approval function?

Q16. Do you agree that a general provision providing for the functional equivalence of electronic signatures to handwritten signatures (e.g. section 8) should not contain any reliability requirement?

Q17. Should any laws imposing a signature requirement be clarified by prescribing the requirements as to reliability that should apply to electronic signatures? If yes, please state the legal requirement (e.g. Civil Law Act, section 6) and describe the standard that should be required of electronic signatures in order to satisfy that legal requirement.

[358] See Australian Commonwealth Electronic Transactions Act 1999 and New Zealand Electronic Transactions Act 2002. Also Canadian Uniform Electronic Commerce Act.
[359] See draft sections 9(1)(d) and 9A(1)(c) in Annex A.

Q18. What difficulties or benefits do you foresee if the provisions of article 9(4) and (5) of the draft convention (relating to originals) are adopted in the ETA?

Q19. Do you have any comments on proposed section 9A in Annex B? Do you agree with the criteria for acceptance of electronic originals in proposed section 9A(1) and (2) in Annex B?

Q20. What difficulties or benefits do you foresee if the provisions of Article 10 of the draft Convention (relating to time and place of dispatch and receipt of electronic communications) are adopted in the ETA?

Q21. What difficulties or benefits do you foresee if the provisions of Article 11 of the draft Convention (relating to invitation to make offers) are adopted in the ETA?

Q22. What difficulties or benefits do you foresee if the provisions of Article 12 of the draft Convention (relating to automated message systems) are adopted in the ETA?

Q23. What difficulties or benefits do you foresee if the provisions of Article 14 of the Convention (relating to Error in Electronic Communication) are adopted in the ETA?

Q24. What exclusions from the applicability of the Convention do you propose in the context of Singapore? Please specify legislative provisions affected where relevant. (See paragraphs 5.16.9 to 5.16.11)

Q25. Do you agree that Singapore should not adopt any of the limitations in article 18(1)? (See paragraph 5.16.12)

Q26. Should sections 13, 14 and 15 in Part IV of the ETA be allowed to apply to non-contractual transactions? (See Part 5.17.1 to 5.17.3)

Q27. Do you have any comments on whether any of the provisions of the Convention should apply to non-contractual transactions? (See Part 5.17.4 to 5.17.7)