Joint IDA-AGC Review of the Electronic Transactions Act

Stage III: Remaining Issues

Submissions

Introduction

1. This is a short note which we have drawn up in response to the request for feedback regarding the Consultation Paper issued pursuant to Stage III of a Joint IDA-AGC Public Consultation exercise on the Review of the Electronic Transactions Act ('Paper'). This note represents our personal views and in no way represents the views of the National University of Singapore, where we teach, nor the views of AGC, where we are Law Reform Consultants.

2. We should also note that we were members of the Electronic Commerce Hotbed Study Group on Legal, Regulatory and Enforcement Issues set up by AGC in 1996 that considered and proposed the enactment of the ETA.

3. We will attempt to address all the questions that have been posed in the Paper. All references to Questions and Paragraphs will be to the same in the Paper. Likewise, all abbreviations that are used in this note correspond to the same abbreviations used in the Paper. All references to Articles in the UNCITRAL draft Convention on the use of electronic communications in international contracts are to the version of the draft dated 12 July 2005.

Regulation of Certification Authorities

4. **Question 1** of the Paper seeks comments as regards the proposal to move technology specific details in the ETA to the ETR. The rationale behind this is to "accord the same benefits to other new and developing technologies like biometrics."[1] Yet the Paper itself notes that the ETA is "generally drafted to be technology

[1] Paper, para. 2.6.3.

neutral… [although] some of its provisions are tied to the definition of secure digital signature [sic], which is PKI specific."[2] The technology specific provisions in the ETA are identified as those in Parts VI, VII, VIII and IX of the ETA.[3]

5. There is no objection to a policy exercise to confine the primary legislation to a description of policy objectives and the subsidiary legislation in the form of ETR to a prescription of the implementation details. Technology neutrality would apply to the formulation of these policy objectives, but it should not be treated as a guide to drafting regulations that implement these objectives, because regulations have to be in many respects specific (if not technology specific) to ensure certainty in their application. For instance, Part VI of the ETA sets out the policy objective, that a special class of signatures (digital signatures) that comply with various security, technical and regulatory requirements will have various legal effects (as regards the integrity of a document signed with a digital signature,[4] and the authenticity and reliability of such digital signatures[5]). Likewise, Part VII of the ETA sets out legal duties that have to be observed by both the CA as well as the putative subscriber of a certificate issued by the CA, and non-compliance with these duties carries criminal sanctions.[6] These form the pre-requisite to a reliable PKI and the policy objectives should not be detracted from.

6. Perhaps Parts VIII and IX of the ETA, which set out detailed technical and administrative duties that have to be observed by the CA and the subscriber, may contain provisions which are more suitable for transfer to the ETR. But it behooves the legislators to have provisions in the ETA that describe the policy behind Parts VIII and IX, which is that CAs and subscribers have legal obligations to ensure that PKI systems are and remain trustworthy: in the case of CAs, to operate trustworthy PKI systems, and administer them in a manner that promotes trust and proper reliance on

---

2 Paper, para. 2.6.1.

3 Paper, question 1, footnote 10.

4 ETA, s 19.

5 ETA, ss 20, 22.

6 *See* ETA, ss 25, 26.

such systems,[7] and in the case of subscribers, to exercise proper care and control and manage their private keys (or for that matter, any biometric indicia) properly,[8] and to timeously inform CAs, repositories and other parties relying on such keys or biometric indicia in the event that such keys or indicia are compromised.[9]

Licensing vs Accreditation

7. It would appear from the Paper that the current regime in the ETA is one of "licensing" CAs, albeit a "voluntary licensing" regime, as opposed to "accreditation" of the CAs.[10] "Accreditation" is defined in the OED as "the action of accrediting; the fact of being accredited; recommendation to credit or to official recognition", and "licensing" is defined as "to grant (a person) a licence or authoritative permission to hold a certain status or to do certain things". In the ETA, aside from the prescriptions regarding how a CA may be "licensed",[11] there are no substantive differences between the operation of a licensed CA and one that is "unlicensed", except one – that a licensed CA is exempted from any losses that exceed the prescribed liability limit.[12] An "unlicensed" CA can operate in Singapore, and need not comply with the ETR. Otherwise, many Singapore companies would not be able to take out certificates with VeriSign, which is the world's largest PKI operator, and which is certainly not licensed in Singapore by the CCA.[13]

8. As such, it is not clear as to what the IDA intends by proposing that the current "licensing" framework be replaced with an "accreditation" framework (**question 2**), unless by "accreditation", IDA is proposing the scrapping of CCA as a "licensing"

---

7 *See* ETA, s 27.

8 *See* ETA, s 39.

9 *See* ETA, s 40.

10 Paper, paras. 2.7.1-2.7.2.

11 ETR, reg. 3.

12 ETA, s 45.

13 At the date of this submission, the only Copyright Act licensed by the CCA in Singapore is Netrust. *See* IDA, Licensed Copyright Acts in Singapore, *at* http://www.ida.gov.sg/idaweb/pnr/infopage.jsp?infopagecategory=regulation:pnr&infopageid=I1966&versionid=1 (accessed 17 August 2005).

authority and renaming it as an "accreditation" authority,[14] albeit one to whom the "accredited" CAs must pay (reduced)[15] licence fees. But if this change of name will help increase certification activities in Singapore and boost e-commerce in Singapore, we see no difficulties in this approach.

9. As regards the questions posed in the Paper (**questions 3 and 4**) on the general attenuation of various financial criteria and fees for "accrediting" CAs, whether or not these criteria and fees are reasonable will depend on the business models and turnover of CAs, the costs of administering the licensing/accreditation scheme and the cost-recovery policies of IDA. (We have no free access to Netrust Pte Ltd's financial statements to be able to make any informed assessment in this regard, and thus we have used VeriSign's SEC financial statements instead.) For instance, VeriSign reported revenues of US$401 million for the first quarter of 2005, and a net income of US$49 million.[16] An examination of its 10-K SEC filing for December 2004 showed that its Security Services group (responsible for its certification authority operations) booked revenues of US$62.8 million. VeriSign also reported an increase in Web site digital certificate revenue of US$23.5 million.[17] We will only observe that the proposed reduction of financial criteria and fees should be assessed against the CAs financial health and status.

10. The Paper also posed an indirect question (**question 5**) as regards the removal of all requirements for auditing a CA's compliance with the ETA, ETR and licence conditions, and to limit any auditing to a CA's compliance with security guidelines.[18] The Paper also asserts that IDA's ability to enforce the ETA and (revised) ETR for breaches will not be reduced.[19] If no auditing on compliance with the ETA, ETR and licence conditions is carried out, it will be difficult for any accreditation agency to

---

[14] See e.g. Paper, paras. 2.8-2.9 (encompassing questions 3-4).

[15] Paper, para. 2.8.16.

[16] VeriSign, Investor Relations, *at* http://www.verisign.com/verisign-inc/vrsn-investors/index.html (accessed 17 August 2005).

[17] VeriSign, Form 10-K filed 16 March 2005, for the financial period ending 31 December 2004, *at* http://ccbn.10kwizard.com/cgi/convert/pdf/VERISIGNINCCA10K.pdf?pdf=1&repo=tenk&ipage=3337259&num=-2&pdf=1&xml=1&odef=8&dn=2&dn=3 at 52 (accessed 17 August 2005).

[18] Paper, para. 2.10.3.

[19] Ibid, footnote 23.

determine if there are any breaches in the CA's operational and administrative procedures, and in turn, the accreditation agency will lose credibility. Perhaps the question that should be asked is: what utility is served by any accreditation as regards a CA's compliance with operational and administrative procedures. The integrity of a CA and its PKI does not depend solely on compliance with security guidelines.[20] If accreditation is to be done, as is proposed in the Paper, biennially, any disruption to the operation and administration of CAs would be minimized. Since clients (and potential clients) of CAs will be assured by these audits that are done on CAs, there is significant commercial benefit for CAs to allow (and facilitate) such audits. Likewise, confidence in electronic commerce in general and CAs in particular among CA clients and consumers of websites hosted by CA clients will arguably be promoted through more frequent checks on the security and integrity of CAs.

Exemption from Liability for Internet (or Network) Service Providers

11. **Questions 6, 7, 8 and 9** relate to the exemption of ISPs (or more accurately, network service providers ('NSPs')) for "objectionable content or defamatory statements".[21] Unfortunately, the Paper does not identify any other circumstances in which the NSPs may be held liable, before seeking to extend the scope of the exemption. In particular, aside from liability for copyright infringement and for defamation, the Paper did not identify any other causes of action for which a NSP may be made liable. In this regard, a comparison of the existing s 10, ETA with NSP exemption provisions in the laws of copyright and of defamation from the various jurisdictions is less than helpful. It would be more helpful for the Paper to clearly identify the causes of action from which a policy decision has been undertaken to shield the NSPs from liability, before working on the language of the exemption. For instance, some other forms of liability which should be considered include disclosures

---

[20] *See, e.g.* Microsoft Security Bulletin MS01-017: Erroneous VeriSign-Issued Digital Certificates Pose Spoofing Hazard, *at* http://www.microsoft.com/technet/security/bulletin/MS01-017.mspx (accessed 13 July 2005).

[21] Paper, para 3.1.1.

of confidential information (for instance, through security compromises),[22] promoting or facilitating intellectual property infringements,[23] criminal contempt of court through publications that are intended to interfere with or impede the administration of justice,[24] publication of identification information relating to children or young persons concerned in judicial proceedings,[25] publication of seditious,[26] blasphemous[27] or obscene matter, publication of confidential banking and financial information,[28] and publication of erroneous or false information leading to economic or fiscal losses.[29]

12. The solution as proposed by the Paper is to (i) define (and extend) the scope of the s 10 exemption to encompass "network service providers", who are defined to mean "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"[30], and (ii) to extend the scope of s 10 to encompass any "third party material" (by removing the reference in the existing s 10 to "merely provides access").[31]

13. This proposed amendment to s 10 changes the original objective of the section entirely. The original objective was the exemption of criminal and civil liability of the network intermediary in cases where the level of moral responsibility of the network

---

22 *E.g. A-G v Times Newspapers Ltd* [1992] 1 AC 191.

23 For instance, through the use of infringing trade marks on advertisement e-banners provided by the NSP. See Trade Marks Act, s 27(4), subject to the defence in s 27(5).

24 Halsbury's Laws of England, 9(1) *Contempt of Court*, at paras. 421-422.

25 Children and Young Persons Act (Cap 38, 2001 Rev Ed), s 35.

26 Sedition Act (Cap 290, 1985 Rev Ed), s 4(1)(c). As a common law cause of action, *see* Halsbury's Laws of England, 11(1) *Criminal Law, Evidence and Procedure*, at paras. 89-97. Cf. Penal Code (Cap 224, 1985 Rev Ed), s 121B.

27 Also part of the class of common law offences against public order under the general heading of sedition. See also Penal Code, Part XV and the Maintenance of Religious Harmony Act (Cap 167A, 2001 Rev Ed), ss 8, 9.

28 *See* Banking Act (Cap 19, 2003 Rev Ed), s 47.

29 *See Ezra, Weinstein & Co. v. America Online*, 206 F.3d 980 (10th Cir., 2000) [hereinafter *Ezra v AOL*].

30 Paper, para. 3.4.8.

31 Paper, para. 3.4.14.

intermediary for the content is extremely low. Thus, according to the Explanatory Statement in the Electronic Transactions Bill, "The protection under this clause will not apply if the provider *does something more than merely providing access to the third-party material*." (Emphasis added). One could not dissent from the proposition that technology has changed and that we probably need to tweak the provision to make sure that the policy objective covers these new technologies. But the instant proposal goes far beyond that.

14. We note that an intermediary's liability in law is ultimately tied to the level of moral responsibility that society attaches to its actions, in providing or operating facilities for online services or network access. The level of moral responsibility depends on the nature of the liability in question. In matters that call for criminal liability, liability will demand a higher level of moral responsibility than civil liability. Thus, intention is almost always required (with some exceptions such as contempt of court). Within matters that call for civil liability, there is a wide spectrum of responsibility depending on the subject nature of the liability. This may range from intention (e.g., an inducement of breach of another's contract, or fraudulent misrepresentation) to strict liability (e.g., distribution of defamatory materials, subject the defence of innocent dissemination), from actual knowledge (an act that assists in a breach of trust) to constructive knowledge (e.g., possible liability for another's breach of confidence), from negligence (e.g., a primary tortious duty of care to prevent harm caused by third party materials, or primary liability for negligent misstatement in third party materials, negligent misrepresentation through the use of third party material) to innocent misrepresentation (of third party material) (leading to liability to have its own contract set aside).[32]

15. There is virtue in what the Paper describes as the "vertical approach" which we have outlined above, because there is a wide range of policy issues underlying why the level of responsibility has been fixed at different levels for different types of liability. This is particularly so since the basis for liability is different in relation to the different activities of the NSPs as applied to the different causes of action. NSPs are *prima facie* liable for copyright infringement of third party content by way of their

---

[32] *Quaere* whether this is an obligation founded on contract.

participation and involvement in the process of making such infringing content available or accessible (contributory or indirect infringement).[33] NSPs are *prima facie* liable for defamation through their publication of third party defamatory content – to make such content known,[34] even if NSPs have no effective control over the maker of the statements.[35] In such instances, there may be good policy reasons to exempt NSPs from liability for copyright infringement or for defamation, especially if no effective control over such publication or dissemination is possible or feasible, or if the NSPs have acted reasonably.

16. In other instances, liability is strict and the rationale behind, for instance, the absolute prohibition on disclosure of confidential information (such as trade secrets, privileged information, sensitive financial information and children's identification information[36]), or the legal obligation to publish accurate and reliable information obtained from third parties such as prices,[37] market information and bids will be lost if a blanket exemption is granted. Thus, under s 10 as it currently stands, an NSP who provides email intranet services for a law firm will not be liable to the law firm's clients[38] for breach of confidence, loss of privileged information and loss of privacy[39]

---

[33] As amended by the Copyright (Amendment) Act 1999 (Act 38 of 1999) and the Copyright (Amendment) Act 2004 (Act 52 of 2004). Thus the copyright exemptions introduced in Part IXA of the Copyright Act work by necessarily characterizing the types of activities undertaken by NSPs which would lead to such infringing materials being accessed or made available. The defences operate as follows: the greater the degree of involvement of the NSP in this process, the greater is the likelihood that it will be held liable. A hosting NSP will be more culpable than e.g. an ISP who merely provides Internet access to a subscriber to access the same infringing material.

[34] Halsbury's Laws of England, 28 *Libel and Slander*, at paras. 60-62.

[35] This is of course subject to the common law defence of innocent dissemination. Halsbury's Laws of England, 28 *Libel and Slander*, at para. 160. In UK, this defence has been largely superseded. NSPs have an additional defence pursuant to the UK Defamation Act 1996, s 1(3)(c) ("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") and s 1(3)(e) ("operator of or provide of access to a communications system by means of which the statement is transmitted, or made available, buy a person over whom he has no effective control").

[36] Cf. Children and Young Persons Act (Cap 38, 2001 Rev Ed), s 35, read with ETA, s 10(2)(c) (which removes from the scope of s 10, all obligations imposed under any written law).

[37] *See e.g. Chwee Kin Keong & 6 ors v Digilandmall.com Pte Ltd* [2005] 1 SLR 502.

[38] There is some legal debate as to whether a cause of action for breach of confidence is founded in contract or in equity. Note that ETA, s 10(2)(a) ensures that the exemption in s 10 does not operate to exclude NSPs from liability any cause of action founded in contract. So while the law firm may be able to maintain a cause of action against the NSP in contract, the client whose confidentiality and privacy

should there be a security compromise that causes confidential and privileged information communicated via the law firm's email system to be disclosed. This is so even if it is the NSP's negligence or recklessness that caused the security breach.

17. In addition, the current indemnity proposal focuses the scope of the s 10 exemption squarely on the expression "third party material". The absence of precision in this expression will create interpretational difficulties. For instance, if an NSP who sets up a blogging service allows a public subscriber such as Mr Black to create his own blog, can defamatory material posted on, say, a user of Mr Black's blog, be said to be "third party material" vis-à-vis the NSP? Can Mr Black be considered the NSP of his blog since it provides reader feedback services? If so, would a public posting on his blog be considered "third party material", or would that depend on whether he is in a position (or alternatively whether he intends) to exercise some measure of editorial or filtering control over "third party material", or has been involved to some extent in the creation, development or transformation of such "third party material"?[40]

18. While there is some sympathy for the NSP and Mr Black as regards their publication of a defamatory statement by a third party,[41] the sympathies will surely change if the material that is posted is seditious or confidential. The "third party material" rule in its current form in s 10 will also encourage NSPs such as content providers and portals to adopt an "outsourcing" or contracting out approach (wherein the materials presented as part of its electronic resources are actually drawn from third party sources) and a "see no evil" approach.[42] Aggrieved plaintiffs will often be in a

---

have been compromised cannot maintain a similar cause of action other than in equity for breach of confidence.

39 *See Douglas v Hello! Ltd* [2001] QB 967.

40 *See e.g. Carafano v Metrosplash.com, Inc. et al*, 207 F.Supp.2d 1055 (C.D.Cal., 2002); affirmed on other grounds, 339 F.3d 1119 (9th Cir., 2003).

41 Witness the debacle over Mr Philip Yeo and A*Star's actions over the blogger Chen Jiahao's publication of allegedly defamatory accusations by third parties on his blog. See http://singabloodypore.blogspot.com/2005/05/singapore-blogger-apologised.html (accessed 13 July 2005).

42 Which is that NSPs should avoid any form of editorial control or input as regards third party material, even if they could exercise some measure of control. This is to avoid the imputation that they have authored or contributed to these third party materials and are responsible for them. *See Ezra v AOL*, at 985 fn 4.

difficult position to prove that these are not third party materials,[43] since this is a matter that is almost exclusively within the knowledge of the NSP. This will enable NSPs to operate with impunity, with disregard for their gatekeeping responsibilities, even if the NSPs expressly reserve these rights,[44] subject only to whatever piecemeal exceptions that are applicable.

19. The Paper suggests that these concerns can be addressed by the "preservation of controls under the Class Licensing Scheme and the obligations to comply with orders to remove, block or disable access to material".[45] With respect, this is too sweeping an assertion to make. NSPs owe legal obligations to their subscribers and users, and these obligations will vary, depending on the nature of the services provided and the types of information disseminated. The current approach in s 10 can be characterised as "see-no-evil until asked to take down". (While there are some 'gatekeeping' obligations imposed on content providers pursuant to the Class Licensing Scheme, these already weak obligations are narrowly crafted to deal with "prohibited material" such as those that are contrary to public order and sexual and violent material, and are practiced on a "best efforts" basis by the NSPs.[46]) This approach further weakens the gatekeeping obligations on the part of NSPs, and provides no incentives, commercial or legal, for NSPs to exercise any gatekeeping responsibilities (since to do so will suggest that these are not "third party materials"). This approach contrasts unfavourably with s 230(c)(2) of the US Communications Decency Act. For all the faults with s 230 of the Communications Decency Act, at least it encourages some good faith editorial intervention and take-down by the NSPs,[47] who do so to restrict access to or availability of objectionable or harassing content.[48] Likewise, s 1(1)(b) and (c) of the UK Defamation Act 1996 also encourages NSPs as publishers to take reasonable care in relation to the publication of defamatory material, and to exercise

---

43 *See Ezra v AOL*.

44 *See Sidney Blumenthal, et al. v Matt Drudge and America Online, Inc.*, 992 F. Supp. 44 (D.D.C. 22 April 1998)

45 Paper, paras 3.4.22 and 3.6 *et al.*

46 Paper, para 3.1.2, footnote 29.

47 47 USC 230(c)(2).

48 This in effect preserves the legal defence advanced (but not accepted) in the pre-Communications Decency Act decision of *Stratton Oakmont v Prodigy Services* 1995 WL 323710.

caution to avoid being infected with knowledge that the NSPs had caused or contributed to the publication of the defamatory material.[49]

20. The Paper did obliquely suggest that aggrieved parties are not without remedies, since NSPs remain obliged to "remove, block or disable" pursuant to the Class Licensing Scheme and pursuant to court orders.[50] But this is the equivalent of bolting the stable door after the horse has escaped and is cold comfort to those aggrieved by the NSP's actions. Once a trade secret has been leaked onto the Internet, there is no way it can be completely retrieved and all traces of it removed.[51] Although s 10 preserves of a cause of action in contract,[52] this is cold comfort for those aggrieved parties who cannot maintain such a cause of action and can only do so in common law[53] in negligence, defamation and breach of confidence.

21. Likewise, there is no reason to exempt NSPs from all forms of intellectual property infringement except for actions for copyright infringement[54]. Presumably, this is because a separate regime exists in the law of copyright that obliges NSPs to discharge some gatekeeping responsibilities in relation to third party infringing material that they may host, transmit or link to.[55] In contrast, while the US Communications Decency Act, s 230 has been interpreted to provide a blanket immunity for all activities by the NSP, s 230 itself excludes from its indemnity activities by NSPs that carry criminal sanctions, intellectual property infringements and breaches of privacy.[56]

---

[49] The litigation in the case of *Godfrey v Demon Internet* [2001] QB 201 is quite instructive, in that the court ruled, *inter alia*, that the NSP lost its UK Defamation Act 1996 s 1(1) indemnity because it did not act quickly and timeously to remove the offending defamatory post, despite being so informed by the plaintiff. *See* also *Loutchansky v Times Newspapers* [2001] EWCA Civ 1805, [2002] QB 783.

[50] Paper, paras 3.4.22 and 3.6 *et al*.

[51] Witness the litigation surrounding *A-G v Times Newspapers Ltd* [1992] 1 AC 191.

[52] ETA, s 10(2)(a).

[53] ETA, s 10(2)(b) excludes from the scope of its ambit, all obligations "established under any written law".

[54] ETA, s 10(2)(d). This provision was only inserted pursuant to the Electronic Transactions (Amendment) Act 2004 (Act 57 of 2004).

[55] Copyright Act (Cap 63, 1999 Rev Ed), Part IXA.

[56] 47 USC 230(e).

22. All these issues stem from the difficulties in trying to craft a broad "horizontal" (non cause of action specific) exemption for network service providers to cover the whole range of possible liabilities with a blanket indemnity in the proposed s 10. The "horizontal approach" in the original s 10 was acceptable because the indemnity was pitched at a very low level (applicable only to *network service providers* who *merely provide access* to *third-party material*.) It catches a few areas of liability where it could be considered rather harsh to impose liability on anyone, such as strict liability offences and torts. The proposed amendment to s 10 will widen the net of exemption without any consideration of the diverse policy considerations that underlie the different liabilities that an intermediary could be subject to. The "network service provider" will have immunity by virtue of its status. And a challenge may plausibly be mounted against this legislation under the Singapore Constitution for breach of equality without a rational nexus,[57] because its net effect is the creation of an "indeterminate indemnity in the network service provider's dealings with an indeterminate class of people for an indeterminate period of time", to paraphrase a famous judicial quotation.[58]

23. Conversely, is there any concern about exposing NSPs to some measure of legal liability for third party material (however it is defined) hosted on their websites or provided as part of a service? To the extent that NSPs are exposed to some measure of contractual liability, they will be able to contain it via the instrument of exemption clauses, subject always to the strictures of the Unfair Contract Terms Act[59] and the Consumer Protection (Fair Trading) Act.[60] Where NSPs may be exposed to tortious liability, the rules of causation and remoteness seem to provide adequate protection. There however may be a need to review our laws of defamation to see if they can better protect our NSPs, and also to promote freedom of expression. As for the other causes of action outlined above, there seems to be little reason to exempt NSPs and thereby deprive aggrieved parties of civil redress where the crux of the cause of action is the publication, knowing or unknowingly, of confidential or erroneous information.

---

57 Constitution of the Republic of Singapore (1999 Rev Ed), Article 12.

58 Cardozo CJ in *Ultramares Corporation v Touche* (1931) 174 NE 441 at 444.

59 Cap 396, 1994 Rev Ed.

60 Cap 52A, 2004 Rev Ed.

The strongest case for exemption from liability would be perhaps from some forms of criminal liability such as those involving strict liability.

24. While we would support a legislative exercise in clarifying the scope of the s 10 indemnity, our view is therefore that IDA and AGC should exercise extreme caution before attempting to extend the already broad s 10 exemption any more than is absolutely necessary. If the net of exemption is to be widened, we favour a functional approach. At least the exemption will be based on the types of actions of the intermediary, and the legislation will prescribe the level of moral responsibility of the intermediary for the actions concerned, explicate the rationale for exempting the intermediary on the basis of those kinds of actions, and provide a rational nexus for the specific exemptions in question.

Electronic Government

25. The proposed changes to ETA s 9 are a step in the correct direction, in that they seek to harmonise all the administrative requirements that are imposed by the different government agencies as regards the retention of electronic records. In response to **Question 10**, these changes are positive and are to be welcomed, subject to three caveats. First, these administrative requirements as imposed in s 9 should be seen to be separate from the evidential requirements (for admissibility of electronic records in evidence) as imposed by the Evidence Act, s 35 (as well as the proposed amendments to s 35). In other words, the imposition of additional requirements must not detract from the fact that such records are legally admissible in evidence. These administrative requirements must therefore not be inconsistent with the evidential requirements, or adversely impact on the admissibility of such records in evidence. Otherwise, businesses will be unnecessarily burdened with having to comply with two sets of legal requirements for the retention of electronic records.

26. Secondly, if such administrative requirements have to be met, they should be gazetted, in the same way as government agencies that seek exemption from the application of s 9. This way, it will be easy for businesses to know how to comply with the proposed s 9.

27. Thirdly, but most importantly, while various e-government initiatives seek to replace physical forms with electronic data entry, it is very important to ensure that the implementation of these electronic forms correspond to the physical forms that they replace, and the administrative and workflow procedures that are in place to deal with these electronic forms are as adequate as, if not more adequate than, the processes for dealing with these physical forms. One of the authors has had some unhappy experiences dealing with the Immigration and Checkpoint Authority's electronic system for submission of various applications, as there were numerous observed discrepancies between the existing "real world" system for submitting applications and the electronic system. In addition, there were ambiguities both in the electronic forms themselves and in the information supplied electronically. There was no access to any proper forum for feedback or for assistance. The "Help" page was under construction. Numerous emails seeking clarification were not acknowledged immediately, and where the responses came, they were less than effective. At the time of making this submission, the author is still waiting for confirmation from the Authority on the status of an application that was made. The move towards an electronic system, which is what the Paper seeks to encourage, should not come at the expense of loss of the high quality of service we have come to expect from government bodies and departments when transposing that same service onto the electronic environment.

28. **Question 11** pertains to revisions to s 47, ETA, to remove any doubts about acceptance by the government of electronic forms containing information, the concern there being whether or not such forms are "records" for purposes of the ETA. The proposal is to revise s 47 to encompass "electronic records or in electronic form".

29. Two observations may be made. First, the definition of an "electronic record" is simply information that is inscribed in electronic medium and *is retrievable*. The emphasis here is in the ability to extract or recover the necessary information that is recorded. In this regard, since there is no doubt that government agencies will be able to retrieve or recover the information that is submitted to them via the various services provided as part of e-government, it is to be doubted if the proposed changes to s 47 will really clarify the law as such. In fact, language such as "by means of electronic records *or in electronic form*" will suggest that information that is processed *need not*

be retrievable, which contradicts the purpose of having some form of record or store of such information.

30. Secondly, if the concern is with the submit-once routed-to-many e-forms, this is very much the scheme of EDI as practised in the public and private sectors. If any substantive changes are proposed to give separate legal recognition to this, the same changes should be made to Part II of the ETA. This was something which was already within the contemplation of the draftsmen of the Model Law on Electronic Commerce.[61]

31. One other pertinent point to note regarding the use of intermediaries to process electronic forms required by Government agencies is that there should be a clear policy that the use of intermediaries does not and will not absolve Government agencies of their legal obligations towards citizens *e.g.* issues of liability for breach of security leading to disclosure of sensitive information submitted in the electronic forms.

32. **Questions 12-14** and the discussion in the Paper deals with the use of "original" documents by Government agencies.[62] While we support the suggestion to have "a single provision on electronic originals instead of many separate provisions to cater to the different situations in which electronic communications are used",[63] there appears to be an overlap in the issue between the use of "originals" as part of the administrative requirements as prescribed by Government agencies, and the use of "originals" in court for admissibility purposes.

33. The later is a rule of law in the Evidence Act[64] which should not be deviated from, even via the imposition of various administrative requirements prescribed by Government agencies. To have different Government agencies prescribe what is an "original" will again lead to a confusion between the administrative requirements for

---

61 *See* generally *Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce* (1996).

62 Paper, paras. 4.11 et al.

63 Paper, para. 4.12.9.

64 Evidence Act (Cap 97, 1997 Rev Ed), s 65. This provision has been the subject of proposed legal reform. Please consult *TLDG*, Computer Output as Evidence: Consultation Paper (September 2003), 127-132 [*TLDG Consultation Paper*].

electronic government and the evidential requirements for legal admissibility. That these two requirements are separate and distinct is best established by comparing Article 9 with Article 10 of the UNCITRAL Model Law on Electronic Commerce.

Proposed UNCITRAL Electronic Contracts Convention and the ETA

34. In answer to **Question 15**, whether or not a signature is used to identify as well as to indicate approval depends on the context in which the signature is used. Where the signature is applied to a contract, as is the case with the draft UNCITRAL Electronic Contracts Convention, Article 9(3), it clearly requires both. In addition, a physical/handwritten signature signifies the signatory's approval of the use of his indicia on that record, and implies his approval of that record. Both approvals are not irrebuttable.[65]

35. As implied in **Questions 16-17**, there is no reliability requirement *per se* of handwritten signatures. But that does not mean that the issue of the reliability of such signatures will never be considered in a court of law. The requirement of authentication of such signatures, as is every item of evidence, will subject signatures to a scrutiny of their reliability. The same requirement of authentication will apply to electronic signatures as well.[66]

36. As for **Questions 18-19** regarding original documents, please refer to the discussions above.

37. As regards **Question 20**, issues regarding time and place of despatch and receipt of electronic messages can never be completely resolved with a simple test of when a message leaves or enters the control of an information system. At best, these rules can only be presumptions which parties may adopt or vary, depending on the circumstances. And the presumptions have to be evidential because notwithstanding the fact that a recipient "becomes aware that the electronic communication has been

---

[65] As for the former, the defence of duress may be pleaded. As for the latter, the defence of *non est factum* may be pleaded.

[66] *TLDG Consultation Paper*, at 92-127.

sent to that address", there may be technical impediments such as the operation of spam filters (for email) or access restrictions that prevent the putative recipient from actually retrieving the message.

38. In line with the principle of technological neutrality, there is no real reason to deem all proposals to the world at large to be considered an invitation to treat. After all, what is or is not an invitation to treat is, as the proposed Article 11 of the draft Convention qualifies, depends on "the intention of the party making the proposal to be bound in the case of acceptance". As such, in answer to **Question 21**, Article 11 adds nothing substantive to the position at common law.

39. In answer to **Question 22**, there is no reason to object to Article 12 of the draft Convention wherein it restates the principle in agency law that a principal is bound by the acts of its agent, which in this case is an "automated message system" which the principal programmed to send out the message in that form, although, presumably, Article 12 will have to be read in conjunction with the ETA, s 13(2)(b).

40. **Question 23** relates to the policy goal of providing some measure of consumer protection for erroneous customer input when contracting electronically. While it may be inspired by the Canadian Uniform Electronic Commerce Act, it also finds form in the EC E-Commerce Directive.[67] In fact, Singapore's ETA should go further and adopt some of these best practices rules as set out in the E-Commerce Directive,[68] for they would encourage good and fair business practices that will have the effect of promoting e-commerce. The only possible objection lies in the language of Article 14(1)(b) of the draft Convention, which states that the recipient has "not used or received any *material benefit* or *value* from the goods or services … received from the other party." (our emphasis) This rule is too strict, since the amorphous term "benefit" is not defined.[69] If the recipient is prepared to make monetary restitution to the vendor

---

[67] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Article 10(1)(c).

[68] Articles 6, 9, 10 and 11.

[69] We note that in the US Uniform Electronic Transactions Act, s 10(2), the reference is only to "benefit", and not "material benefit". We also note that s 10(3) preserves the application of the law of mistake to such an erroneous transaction.

for such “benefit” or usage and the benefit is easily measurable in monetary terms, there is no reason why he should be unable to reverse the transaction. For instance, in many e-commerce contracts today, the consumer is entitled to return a purchased item to the vendor for whatever reason, subject only to shipping charges and a “restocking fee”. The Convention should make provision to encourage this e-commerce practice, which seems to be an equitable way to balance the rights of the e-commerce vendor and the consumer.

41. Another difficulty is that the draft Convention excludes contracts concluded for personal, family or household purposes (Article 2(1)(a)) and most electronic payment systems (Article 2(1)(b)). The applicability of the draft Convention also presupposes in the first instance that the contracting parties have “places of business” in different contracting states (Article 1(1)). These provisions suggest that consumers would not be able to take advantage of the protection in the Convention rules, especially as regards mistakes made in contracts for their personal purposes, and mistakenly made payments. If this is so, then unless this gap is filled within the domestic legislation of Singapore, consumers, who will need this protection the most, will be left out in the cold.

42. We note that **Question 24** pertains to the results of the IDA-AGC Review of the ETA: Exclusions under section 4 of the ETA, to which we are not privy.

43. As regards **Question 25**, it appears from the summary of the relevant provisions in the Paper, in particular, the possible reservations under Article 19(1), that the Convention is intended to apply to all transactions falling within its scope, irrespective of the rules of private international law of the forum. While such an approach will lead to greater certainty from the forum’s perspective, we urge caution at this stage. Generally, the domestic law of the forum should only apply if the law represents some fundamental public policy of the forum, protecting some essential moral, social, or economic interest of the forum. Otherwise the application of the law of the forum may be unjust to the parties in particular disputes. For instance, let us have a situation where party A in country X allegedly enters into an electronic contract with party B in country Y, and X and Y are not signatories to the Convention, but have a bilateral treaty containing rules governing the formation of such contracts. Assuming that the Singapore court is hearing the case, it does not appear to be fair to

apply the rules in the Convention to such a case. The problem may not be a practical one if the rules in the Convention gain universal or near-universal acceptance, so that the efficiency gains in the straightforward application of the Convention rules would outweigh the costs of applying choice of law in all cases and the potential injustice of not applying choice of law in the odd case. Unless we are very confident of the universal or near-universal adoption of the Convention rules, the more cautious way to proceed would be to apply the reservations in Article 19(1) at the first instance.

44. As regards **Questions 26** and **27**, we would agree that Part IV of the ETA should apply to non-contractual transactions. Likewise, provisions pertaining to the legal recognition of electronic records, legal requirement for writing, and electronic signatures should apply to non-contractual transactions.

Conclusions

45. We thank IDA and AGC for the opportunity to comment on these issues in the ETA, and we hope that our observations in this short note will prove to be useful.

(digitally signed)
Daniel SENG
Associate Professor
Faculty of Law
National University of Singapore
13 Law Link
Singapore 117590
17 August 2005

(digitally signed)
YEO Tiong Min
Associate Professor
Faculty of Law
National University of Singapore
13 Law Link
Singapore 117590
17 August 2005