A REVIEW OF IT LAW DEVELOPMENTS IN SINGAPORE

Joyce A. **TAN**
LLB (Hons) (NUS)
Advocate & Solicitor (Singapore), Solicitor (England & Wales)

Daniel **SENG**
LLB (NUS), BCL (Oxford)
Advocate & Solicitor (Singapore)
Associate Professor, Faculty of Law, National University of Singapore.

Singapore's aspiration to be a centre for IT and electronic commerce has been on the back of the proactive efforts at developing IT law here, keeping in pace with changes and trends in technology. This paper seeks to conduct a critical review of these relevant laws. It will selectively focus on the areas of cybercrimes, electronic commerce, data protection, electronic money, domain names and open source, where there have been a number of interesting legal or policy initiatives or technical developments, national and global, and where Singapore can seek leadership status in the global marketplace for IT infrastructure and legal services.

I. Introduction

1 Singapore has one of the highest IT literacy and penetration rates in the world. The most recent survey by the Info-communications Development Authority of Singapore ('IDA') shows that as of September 2005, 49.8% of all households have broadband access, whereas Internet dial-up usage stands at 38.9%. Mobile phone penetration stands at 98.7%.[1] Likewise, the overall usage of info-communication appliances in businesses is very high, standing in a 2004 survey at 83%.[2] The Singapore Government has aggressively enhanced and promoted the development of IT infrastructure of the country.

2 And with national plans to make Singapore an "intelligent island" also comes the need to put in place and upgrade the necessary legal infrastructure to support this IT infrastructure.[3] Singapore has found itself placed on the global stage in this regard. For instance, Singapore is the first country in the world to implement the UNCITRAL Model Law on Electronic Commerce. It is also heartening to know that its Electronic Transactions Act has been in turn the model law upon which other countries have enacted their electronic commerce laws. However, just as the only constant in technology is change, we should also be prepared to review and upgrade our legal infrastructure to keep up with changes and trends in technology.

---

1 Infocomm Development Authority of Singapore, *Statistics on Telecom Services for 2005 (Jul - Dec)*, <http://www.ida.gov.sg/idaweb/factfigure/infopage.jsp?infopagecategory=factsheet:factfigure&versionid=1&infopageid=I3558> (accessed 2 November 2005). Singapore has been rated by the Global information Technology Report 2004-2005 as the world's most network ready country, with the United States ranked in fifth position. *See* <http://www.weforum.org/pdf/Global_Competitiveness_Reports/Reports/GITR_2004_2005/Networked_Readiness_Index_Rankings.pdf> (accessed 29 October 2005).

2 Infocomm Development Authority of Singapore, *Survey on Infocomm Usage in Businesses for 2004*, at <http://www.ida.gov.sg/idaweb/doc/download/I3559/IT_Usage_2004_Exec_Summary_250805.pdf> (accessed 2 November 2005).

3 *See, e.g.*, Minister for Home Affairs (Mr Wong Kan Seng), Parliamentary Debates: Second Reading of the Computer Misuse Amendment Bill 1998 (30 June 1998), Parliamentary Debates, at col 390.

II. Cybercrimes and Electronic Fraud

3 Singapore was one of the first countries in the world to enact legislation to deal with cybercrimes. Nevertheless, the Computer Misuse Act,[4] enacted in August 1993 and modelled on the UK Computer Misuse Act, has not stood still. To keep up with new incidents of cybercrimes and new forms of technological risks, the Computer Misuse Act has since been extensively revised, once in 1998[5] and recently in 2003.[6]

A. The Computer Misuse Act

4 Recent local jurisprudence, which is sparse, has helped in the interpretation and application of the Computer Misuse Act. The operative element in most of the penal provisions in the Computer Misuse Act is "without authority" or lack of authorization.[7] With one exception, to be discussed later in this Paper, a Computer Misuse Act offence is made out if the accused commits the activity in question without authorization, and does so "knowingly".[8] Of course, the Chief Justice's suggestion in *PP v Muhammad Nuzaihan bin Kamal Luddin* that "the courts may well have to apply the principles of strict liability so that the offender's state of mind was irrelevant to a finding of guilt"[9] should be understood in its proper context. The accused in *Muhammad Nuzaihan bin Kamal Luddin* was charged with the offences of unauthorized access, unauthorized obtaining of a computer service and unauthorized modification. He claimed that he did not have the requisite guilty intent; his only intention in accessing without authority the systems in question was "to check for vulnerabilities". The Chief Justice was rightly dismissive of this defence, noting that the facts suggested that the accused had made a conscious decision to apply his hacking skills, and also subsequently bragged about his exploits on the Internet Relay Chat (IRC). Thus the decision in *Muhammad Nuzaihan bin Kamal Luddin* actually affirms that the *mens rea* element for a Computer Misuse Act offence is indeed present, and has to be established objectively, and not the offender's *actual* state of mind. An accused cannot claim that he did not have the requisite *mens rea* simply because the compromised systems had well-known vulnerabilities and he was merely seeking to test them for these vulnerabilities.

B. The Meaning of "Authorisation"

5 The meaning of the expression "without authority" received judicial treatment in *Lim Siong Khee v PP*,[10] where the Chief Justice, applying the House of Lords decision in *R v Bow Street Magistrates' Court, ex parte Allison*,[11] held that the Computer Misuse Act is not concerned with authority to access *per se*, but with authority to access the actual data and programs concerned. In so doing, the Chief Justice rightly held that a person who had been given authority to help the account holder access an email account while overseas, does not have any authority to access that account for any other purpose.[12] Likewise, a systems administrator who maintains email accounts has no authority to access an account holder's email account, since whether access is with authority depends on the account holder.[13]

---

4 Act 19 of 1993 (Cap 50A, 1994 Rev Ed).

5 Computer Misuse (Amendment) Act (No 21 of 1998).

6 Computer Misuse (Amendment) Act (Act 25 of 2003).

7 Computer Misuse Act, section 3 (1) ("unauthorized access"), section 5(1) ("unauthorized modification"), section 6(1) ("unauthorized use or interception"), section 7(1) ("unauthorized obstruction"), section 8(1) ("unauthorized disclosure").

8 *Id*.

9 [2000] 1 SLR 34 at 19.

10 [2001] 2 SLR 342.

11 [1999] 4 All ER 1.

12 *Lim Siong Khee*, *supra* n 10, at 19.

13 *Id* at 14.

6 *Lim Siong Khee* thus has greatly clarified the law as regards the scope of authorisation under the Computer Misuse Act. By giving the account holder the superior right to regulate access to his email account, to the exclusion of even the systems administrator or the Internet Service Provider, *Lim Siong Khee* has afforded the user with a fair measure of protection against any possible intrusion into his privacy. Of course, the analysis may be different as regards email accounts maintained by the employer in the course of work, as opposed to the personal email account in *Lim Siong Khee*. It is noteworthy that the Chief Justice in *Lim Siong Khee* was even prepared to rule against a systems administrator, who has overall technical access to all accounts on a mail system. The scope of authority is thus determined by a complex amalgam of the nature of the account (whether it is for the course of work or for personal purposes), the nature and terms of use (whether the person who is so entitled to grant authority[14] overall has passed on that authority or a subset of it to the end user), the regularity or irregularity of such uses and the peculiar circumstances (e.g. an ethical hacker has implied authority to test a system for vulnerabilities, but his authority may be circumscribed by his obligation to nonetheless protect the integrity of the critical components of the system and his duty to the systems administrator to disclose the results of his test). *Lim Siong Khee* thus makes it imperative for those who access or otherwise use accounts other than in the normal course of events to secure authorisation in writing from authorised persons to confirm their legitimate access or use. Yet the court should also pay heed to the warning in *Bow Street Magistrates* that a Computer Misuse Act offence of lack of "authorisation" committed by an "insider" accused should only be made out if the accused had exceeded the clearly defined limits of his authority, which the accused "*should know*".[15] Thus the *mens rea* element will engage the *actus reus* element in delimiting the scope of a Computer Misuse Act offence.

7 In this regard, section 4 of the Computer Misuse Act stands out as an aberration. The offence of aggravated hacking is constituted when an accused accesses a computer with intent to commit an offence involving property, fraud, dishonesty or which causes bodily harm. Prior to the 1998 amendments, the access in question must be unauthorized access. But the 1998 amendments removed this requirement for the access to be unauthorized. In Parliament, in moving the amendments, the Minister referred to an instance where employees of a cinema accessed the cinema's cash card computer to top up unused cards for subsequent sale and altered the computer to cover their tracks.[16] The employees were prosecuted under the Penal Code for criminal breach of trust. The Minister seemed to opine that but for the fact that their access to the computer was authorized, the employees could be prosecuted under section 4 of the Computer Misuse Act.

8 Of course, this narrow reading of the concept of "authorization" was prior to the case of *Bow Street Magistrates*. If it could be established that the cinema did not allow its employees to use the cash card computer to top up unused cards, their access to the computer would be unauthorized and the offence of aggravated hacking under section 4 would be made out. In any event, the employees had clearly committed the offence of criminal breach of trust by defrauding the cinema, their employer. However, the present section 4 as amended by the 1998 amendments has the jurisprudential effect of making an offence involving property, fraud, dishonesty or which causes bodily harm additionally punishable because a computer was used. This can give rise to awkward scenarios. For instance, an accused will be liable for robbery, regardless of whether he found his way around the neighbourhood through experience or used a physical street directory to plan his targets. If he had instead used an electronic map or street directory for this purpose, he would be additionally liable under section 4 of the Computer Misuse Act. This is so even though there was no "misuse" of the computer whatsoever that led to the commission of his offence. If it was not Parliament's intention to create a "computer-oriented" offence that would aggravate any offence as long as a computer was used, in the light of the clarification of the law in *Lim Siong*

---

14 Computer Misuse Act, section 2(5)(b), (8)(b).

15 *Bow Street Magistrates*, *supra* note 11, at 9.

16 Minister for Home Affairs (Mr Wong Kan Seng), Parliamentary Debates: Second Reading of the Computer Misuse Amendment Bill 1998 (30 June 1998), Parliamentary Debates, at col 390.

Khee in 2001, where *Bow Street Magistrates* was accepted, perhaps the 1998 amendments to section 4 should be reversed.

C. Other Provisions in the Computer Misuse Act

9 A review of the Singapore edition of its Computer Misuse Act will be incomplete without some mention of some of its idiosyncrasies.

(1) Securing Access Without Authority

10 The first relates to the offence of "securing access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service" in section 6(1)(a), with which the accused in *Muhammad Nuzaihan* was charged. It is noteworthy that in the one charge where the prosecutor chose to proceed against the accused in *Muhammad Nuzaihan* under section 6(1), the charge was framed as relating to the accused accessing a port of the server the accused had compromised to gain access to a communications service. On the facts of *Muhammad Nuzaihan*, this pertained to the functionality described as Internet Relay Chat.

11 There is a clear overlap between this section and section 3, which relates to the offence of "securing access without authority to any program or data held in any computer". While section 3 is adapted from the original UK Computer Misuse Act, section 6(1) is taken from the Canadian Criminal Code.[17] The focus of section 3 is on the program or data which the accused had accessed without authority, but the focus of section 6(1)(a) is on accessing the computer and obtaining a functionality. Since any computing functionality is produced via programs and data, it is conceivably possible to frame any section 6(1)(a) charge in the language of section 3.[18] The language of section 6(1)(a) is also apt to lead to confusion, since it emphasizes the now-disavowed approach[19] of establishing the lack of authorization to access the computer, rather than to obtain the computer service. It is noteworthy that the current version of the provision of the Canadian Criminal Code now emphasizes the absence of right to obtain the computer service, rather than access to the computer. Thus it is submitted that the presence of section 6(1)(a) in our statute books is duplicitous and will interfere with the interpretation of section 3. It should be repealed.

(2) Protected Computer

12 Another idiosyncratic innovation is section 9, which introduced the concept of a "protected computer", via the 1998 Computer Misuse (Amendment) Act. This provision seeks to enhance the penalties of an offender guilty of an unauthorized access offence (section 3), an unauthorized modification offence (section 5), an unauthorized use or interception of a computer service offence (section 6) and an unauthorized obstruction offence (section 7), where the attacked computer falls into a special class of computers that are considered more critical or vulnerable. It is obviously inspired by the "protected computer" provision in section 1030(e)(2) of the US Computer Fraud and Abuse Act. However, its implementation in section 9, which has yet to be judicially considered, is fraught with difficulties.

13 First, section 9 is not automatically triggered if the accused compromises a "protected computer". It has to be shown that the accused knows or ought reasonably to have known that:

> the computer or program or data is used directly in connection with or necessary for —
>
> (a) the security, defence or international relations of Singapore;

---

17 Canadian Criminal Code, Chap C-46, Statutes of Canada, Part IX (Offences against Rights of Property), section 342.1(1)(a).

18 Canadian Criminal Code, section 342.1(2) (defining "computer service" as including data processing and the storage or retrieval of data).

19 The approach of examining the access to the computer to determine if the access is "without authority" was disapproved in *Bow Street Magistrates*, *supra*, note 11, where the House of Lords in effect overruled the English High Court decision that so held in *DPP v Bignall* [1997] Info TLR 168.

(b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;

(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or

(d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services.[20]

14 Because of the knowledge requirement, the fact that this is a "protected computer" has to be brought to the knowledge of the accused. Thus section 9 additionally provides that "if there is, in respect of the computer, program or data, an electronic or other warning exhibited to the accused stating that unauthorised access to that computer, program or data attracts an enhanced penalty under this section", it shall be presumed that the accused had the requisite knowledge.

15 This introduces a question of its practical utility. A legitimate user who accesses a computer system does so via a known and predictable route. The electronic warning may be inserted and exhibited along this route so that the user will see the exhibition in the course of using the system. But a hacker who attacks a system will not do so via this predictable route, and will clearly not see, and has no intention of seeing, any such electronic warning or prompt. Furthermore, it is difficult to see how an electronic warning can be embedded in data without triggering any recoding or interfering with existing code and data.

16 Secondly, a close analysis of section 9 shows up several inconsistencies in legislative intention. The operative provision, section 9(1), states that "*access* to any protected computer" has to be obtained pursuant to the commission of a section 3, 5, 6 or 7 offence. The application of section 9 to section 3 (unauthorized access) seems straightforward, save for the observation that the section 3 offence is predicated, not on access to *a computer*, but to *programs or data* stored on a computer. Section 9(2) elaborates that knowledge that the programs or data is used directly in connection with the critical purposes will render the computer housing the programs or data that is accessed a protected computer. Perhaps this will resolve this legislative incongruity.

17 However, sections 5, 6(1)(b), 6(1)(c) and 7 are not predicated on *access* to a computer. It could be argued that this is due to a problem in legal drafting, and that the element of "access" need not be strictly satisfied. Yet there are indeed conceptual difficulties in the application of a protected computer to these offences. For instance, an accused may do an act such as to release a computer virus which he knows will cause an unauthorized modification of the contents of any computer (section 5). Can he contend that he does not know, or has no reasonable belief that the programs or data of a protected computer will be modified by his act? Indeed, section 5(3) states that it is immaterial for the section that the act in question is not directed at any particular program, data or computer. Nonetheless, section 9 seems to require some specific level of knowledge, objectively construed, connecting the act in question to the protected computer – that "the computer or program or data is used directly in connection with or necessary for" the protected purposes.

18 Likewise, the same could be said of the proscribed activities in sections 6 (unauthorized interception) and 7 (unauthorized obstruction) by testing these activities against the "electronic warning" requirement. How would an accused have knowledge of this electronic warning if he has released a virulent virus that propagated through diverse channels before eventually attacking a government computer (a section 5 offence of unauthorized modification), or when he has intercepted some electronic communications between government officers which he happened to pick up when listening for unencrypted communications from unprotected access points (a section 6 offence of unauthorized interception), or when he floods HDB's email server with so much email[21] that any official communications between HDB and a critical government Ministry is disrupted (a section 7 offence of unauthorized obstruction)? If the accused knows that the

---

[20] Computer Misuse Act, section 9(2).

[21] *See, e.g., PP v Kendrick Tan* at http://mishpat.net/cyberlaw/archive/cyberlaw50.shtml.

computer in question is a protected computer subsequent to the time of the commission of the offending act in question, but not before, is this *ex post facto* knowledge relevant?

19 In contrast, under the US Fraud and Abuse Act, it is reasonably clear that the onus is on the prosecution to prove that the compromised computer was used exclusively by a financial institution or the US Government, or where the conduct in question affects such a use by a financial institution or the US Government, or where the computer was used in interstate or foreign commerce or communications.[22] This formulation avoids all complications regarding knowledge about the protected computer, and seems preferable to the existing formulation in section 9 of the Computer Misuse Act.

D. Electronic Fraud and Other Crimes

20 A general observation that can be made about the Computer Misuse Act is that it contains numerous forward looking provisions, particularly those dealing with unauthorized access, unauthorized interception and unauthorized obstruction of the use of computers. However, the focus of the Computer Misuse Act is about protecting the integrity of computing infrastructure. It contains no provisions that deal with other types of criminal activities that have arisen with the proliferation and the widespread accessibility of the Internet.

21 Many of these are dishonest practices and activities peculiar to the electronic commerce environment. Unlike the proscribed activities set out in the Computer Misuse Act, many of these dishonest practices can be carried out by people without technical skills or the necessary technical competence. While many of these practices can be successfully prosecuted under existing laws such as cheating, theft and criminal breach of trust under the Penal Code, many other activities do not fall within the ambit of the Computer Misuse Act or do not fall exactly within existing provisions in the Penal Code. One of the authors has written a joint paper that discusses these issues,[23] and this paper will only contain a summary of that paper.

22 One of the most significant problems in the electronic environment, particularly in the electronic commerce environment, is identity theft. This occurs when an unauthorized person uses a victim's personal information such as his identification number, credit card number or some other form of identifying information to execute a transaction or make a purchase. After acquiring the good or benefiting from the service, the perpetrator disappears, leaving the innocent victim to dispute the transaction or purchase which he has ostensibly concluded.

23 While the perpetrator may be prosecuted for cheating, this Penal Code offence only addresses the criminal consequences of the theft of identity, and not the act of "theft" of the identity itself. It is seriously doubted if "identity theft" per se is an offence under our existing criminal laws. The Penal Code provisions on "theft" and "dishonest misappropriation of property" both require that the subject of the "theft" or "misappropriation" be "movable" property in "tangible form". This is affirmed by the clear common law decisions that have held that information *per se* is not "property" and cannot be stolen.[24] Nor does section 8 of the Computer Misuse Act offer much help: it is limited to the disclosure of passwords, access codes or other means of gaining access.

24 This is not an appealing result, especially since identity information may be dealt with without using such stolen identity information to commit theft or cheating offences. Underground hacker communities exist to exchange compromised identity information, to trade in such information for other benefits. Such activities severely compromise the security and confidence in e-commerce systems, particularly payment systems. Of course, credit card companies have

---

22 US Computer Fraud and Abuse Act, section 1030(e)(2).

23 Daniel Seng and Sriram Chakravarthi, *E-commerce Fraud in Singapore – A Legal Review*, (April 2004 and August 2004), CAD Chronicle.

24 *Oxford v Moss* (1979) 68 Cr App R 183; *R v Stewart* (1988) 50 DLR (4d) 1.

responded by issuing special authentication tools to validate credit card numbers and the e-commerce transactions conducted with them. Surely it is imperative that the legal infrastructure supports this initiative by criminalizing the activities of identity theft and trade in identities.

25 In this regard, there is much utility in having *sui generis* legislation to deal with the problem. Section 1028(a)(1) of the US Identity Theft and Assumption Deterrence Act makes it an offence to "knowingly and without lawful authority [produce] an identification document or false identification document". Sections 1028(a)(2), 1028(a)(3), 1028(a)(4), 1028(a)(6) and 1028(a)(7) make it an offence to, among others, possess identification documents with a view to their transfer, use or for defrauding others, or to knowingly transfer or use such documents without any lawful authority to commit a criminal offence. Thus US law crminalises all activities relating to identity theft such as the appropriation, possession, transfer and use of misappropriated personal identities. It may be apposite for our authorities to consider this approach with a view to updating our criminal laws to plug this obvious lacuna.

III. Electronic Commerce & E-Government

26 When the Electronic Transactions Act ("ETA")[25] was enacted by Parliament in June 1998, it was done against the backdrop of a legal environment uncertain about the application of existing laws to the electronic environment. The paradigm of the ETA was to confirm the applicability of existing contract laws to transactions concluded electronically. Thus rules confirming the enforceability of information in the form of electronic records,[26] electronic writing,[27] electronic signatures,[28] electronic evidence,[29] electronic offers and electronic acceptances[30] as well as electronic invitations to treat[31] received first treatment in the ETA. The fact that these issues are now uncontroversial is evidenced by the recent case of *SM Integrated Transware Pte Ltd v Schenker Singapore Pte Ltd*[32], where email communications between the landlord and prospective tenant were held sufficient to constitute the requisite writings to evidence a lease, outside of the ETA. As Prakash J said:

> The ETA does not change the common law position in relation to s 6 of the [Civil Law Act]. Whether an e-mail can satisfy the requirements for writing and signature found in that provision will be decided by construing s 6(d) of the [Civil Law Act] itself and not by blindly relying on s 4(1)(d) of the ETA.[33]

A. Exemption of Network Service Providers

27 The next most substantive part of the ETA relates to the section 10 exemption from legal liability of network service providers for merely providing access to third-party material.[34] This broad exemption with limited exceptions was based on the German Multimedia Act.[35] The language of section 10 has been criticized as too vague and imprecise, since the terms "network service provider" and "merely providing access" are not defined in the section. In response to these criticisms, in the AGC-IDA Consultation Paper on Electronic Contracting Issues – Stage III: Remaining Issues,[36] AGC and IDA have proposed further broadening the section 10 exemption by

---

25 Cap 88, 1999 Rev Ed.

26 ETA, section 6.

27 ETA, section 7.

28 ETA, section 8.

29 ETA, section 9.

30 ETA, section 11.

31 ETA, section 12.

32 [2005] SGHC 58, [2005] 2 SLR 651.

33 *Id* at 76.

34 ETA, section 10.

35 German Federal Law to Regulate Conditions for Information and Communication Services, Art 1s5.

36 Consultation Paper – Joint IDA-AGC Review of [the] Electronic Transactions Act– Stage III: Remaining Issues (22 June 2005)

extending it to apply to content providers. A detailed review and analysis of section 10 was provided by one of the authors of this paper in a submission to AGC and IDA.[37] This analysis is summarised here as follows. The concern is that the existing section 10 and the proposed section 10, are formulated on the basis of a broad "horizontal" (non cause of action specific) exemption for network service providers purportedly covering the whole range of possible liabilities. Such a broad horizontal exemption does not take into account the diverse policy considerations and moral responsibilities that underlie the different liabilities that a network service provider ought to be accordingly subject to. As it currently stands, the exceptions to the existing and proposed section 10 exemption (whereby the network service providers are exposed to liability in respect of any obligation founded in contract, imposed under a licensing or regulatory regime or under any written law or by a court to remove, block or deny access to any material and any liability arising from any copyright or related-rights infringement)[38] are crafted in a piecemeal fashion and the rationale for the existence of each exception (and the denial of other liabilities such as that for defamation) are not readily explicable.

B. Electronic Signatures and Electronic Communications

28 The bulk of the ETA is taken up by provisions dealings with the legal efficacy of electronic signatures and electronic communications, in particular, the legal efficacy of a special class of electronic signatures – digital signatures – and the public key infrastructure required to support digital signatures.[39] Most of these provisions were derived from the Illinois Electronic Commerce Security Act and the Utah Digital Signature Act, and in the AGC-IDA Consultation Paper on Electronic Contracting Issues – Stage III: Remaining Issues, AGC and IDA have proposed transferring most of these provisions to subsidiary legislation to "accord new authentication technologies the same benefits as those currently enjoyed by [Public Key Infrastructure] quickly and conveniently by enacting new regulations"[40]. Many of the technical provisions in the ETA form the pre-requisite to a reliable Public Key Infrastructure since they set out the minimum legal duties that have to be observed both by the certification authority as well as by the subscriber of a certificate issued by the certification authority. While the proposal to move these technology-specific provisions to subsidiary legislation is of itself not a concern, the authors here also note that the limited size of Singapore may discourage competition so that only one or a few providers of digital signature or other forms of authentication services may dominate the market. In such a scenario, there is a role for legal intervention to prescribe minimum standards of compliance to promote reliability and confidence in digital signatures or other authentication systems to prevent the service providers from themselves setting the benchmarks, and to do so with sufficient scalability to accommodate changing technology. 29 The difficulty with reforming this area of the law relating to electronic contracting is that electronic contracting law rests on the very well established jurisprudence of contract law. As the case of *SM Integrated Transware*[41] has illustrated, contract law is as malleable and as adaptable as the circumstances to which it is applied. Very good policy reasons must be offered if the jurisprudence as applied to electronic contracts were to develop differently from real-world contracts, particularly through legislative intervention. This is especially so since one of the cardinal principles embodied in electronic contracting laws such as the ETA is the principle of equivalence. The principle of equivalence recognizes that with the prevalence of electronic contracts, the divergence of jurisprudence will lead to an undesirable schism not just in the law but also in the acceptance of electronic transactions.

<http://statutes.agc.gov.sg/agc/Publications/ConsultnPap/ETA_StageIII_Remaining_Issues_2005.pdf> (accessed 28 December 2005).

37 Daniel Seng and Yeo Tiong Min, *Submissions: Joint IDA-AGC Review of [the] Electronic Transactions Act – Stage III: Remaining Issues* (17 August 2005), at 11-24.

38 ETA, section 10(2).

39 ETA, Parts V-X.

40 *Supra* n 36, at para 2.6.4.

41 *Supra* n 32.

30 However, where the law as it currently stands impedes the growth and development of electronic commerce, there is much to commend for an update of the law. From this perspective, the market acceptance of digital signatures and indeed other authentication technologies will be facilitated if vendors and consumers can be assured that the implementations of digital signatures and such authentication technologies in the marketplace have complied with the prescribed legal safeguards.

C. Consumer Rights

31 With the basic laws of electronic commerce in place and the increasing maturity of the e-commerce market, it is submitted that it is time for us to focus our attention on making the domestic e-commerce market a reliable and trustworthy one. The growing need for us to protect the interests of consumers is evidenced by the recent enactment of the Consumer (Fair Trading) Act. This piece of legislation supplements the growing pool of other consumer-protection legislation such as the Consumer Protection (Trade Description and Safety Requirements) Act, the Multi-Level Marketing and Pyramid Selling (Prohibition) Act, the Sale of Goods Act and the Unfair Contract Terms Act by offering consumers protection from and basic redress against vendors.

32 There is also a need to enact similar legislation for the electronic environment. With the growth of the electronic commerce and the ease with which vendors can have an electronic presence, an increasing number of consumers will be exposed to vendors who make false advertisements or representations about their offers, who offer their goods or services only on unreasonable terms and conditions, who have unfavourable terms for payment or who take advantage of the virtual nature of Internet transactions to discourage or even deprive consumers of their rights to return defective goods, ask for refunds or exercise their basic consumer rights which they are otherwise entitled to in the non-virtual environment. The trend towards consumer protection is evidenced in e-commerce legislation in the US, but particularly so in Europe, with the passage of the EU Directive on Electronic Commerce in 2000[42] as well as the EU Distance Selling Directive in 1997[43]. In addition, there are special directives to deal with specialized transactions in medicinal products and financial products. Contrary to the views recently expressed in the local judgment of *Chwee Kin Keong v Digilandmall.com Pte Ltd*,[44] the fact that consumers are exposed to and have access to more information about the products and services that they intend to purchase means that they should be offered more, and not less, legal protection, in order to preserve their confidence in electronic transactions.[45]

33 It is submitted that as regards legal reform, three areas call for particular attention to protect consumers in the e-commerce environment. The first is that there must be means put in place to identify the vendor in the virtual environment. E-commerce vendors should be required to make the following information easily, directly and permanently accessible, not just to consumers to facilitate the consummation of consumer transactions, but also to enable the competent authorities to exercise supervisory oversight over the vendors. Such information would comprise:

(a) The name of the e-commerce vendor;

(b) The geographic address at which the vendor is established;

---

42 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, OJ L 178/1 17.7.2000, 1.

43 Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, OJ L 144, 4.6.1999, 19.

44 *Chwee Kin Keong & 5 ors v Digilandmall.com Pte Ltd* [2004] 2 SLR 594, [2004] SGHC 71.

45 Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directive 97/7/EC and 98/27/EC, OJ L 271/16, 9.10.2002, Recital (3).

(c) The details of the vendor, including its email address;

(d) The trade register in which the vendor is registered and the registration number, if applicable;

(e) The particulars of the relevant supervisory authorities where the vendor's activity is subject to an authorization scheme;

(f) Any other requirements as prescribed by the regulatory authority of which the vendor is a member, and

(g) The GST identification number where the vendor's services are subject to GST.[46]

34 The second area of reform would require the vendor to observe certain standards when providing e-commerce services. In particular, the vendor is required to provide certain basic information relating to the transaction in question. These are the "electronic formalities" that precede the consummation of the transaction. These electronic formalities have been imposed under the US Uniform Electronic Transactions Act 1999 ("UETA"), the US Electronic Signatures in Global and National Commerce Act 2000 ('US E-Sign') as well as the EU Directive on Electronic Commerce, and they require the vendor to, prior to the order being placed by the purchaser, to clearly, comprehensively and unambiguously provide the following information:

(a) The different technical steps to follow to conclude the contract;

(b) Whether or not the details of the concluded contract will be kept by the vendor and whether it will be subsequently accessible;

(c) The technical means for identifying and correcting input errors prior to placing the order; and

(d) The languages offered for the conclusion of the contract.[47]

35 They are required to clearly and unambiguously identify promotional offers as such and the conditions to be met to qualify for them.[48] They are also required to observe the following steps to conclude the contract:

(a) The vendor has to acknowledge the receipt of the purchaser's order without undue delay and by electronic means;

(b) The order and acknowledgment of receipt are deemed to be received when the vendor (or the party to whom they are addressed) is able to access them.[49]

36 Thirdly, the vendor must provide the purchaser with appropriate, effective and accessible technical means to allow him to identify and correct input errors. While the EU legislation requires this remedy to be available to the purchaser prior to the placing of the order,[50] the US legislation goes one step further and requires the vendor to provide a mechanism to enable the purchaser to avoid a transaction that is made as a result of an error by the purchaser, where the purchaser is dealing with the vendor operating an electronic processing system.[51] A similar rule is

---

46 EU Directive on Electronic Commerce 2000, Article 5(1).

47 *Id*, Article 10.

48 *Id*, Article 6(c).

49 *Id*, Article 11; US E-Sign, s 101(c) (as relating to the retention of electronic records), US Uniform Electronic Transactions Act 1999, s 8 (provision of information in writing, presentation of records).

50 EU Directive on Electronic Commerce 2000, Articles 10(1)(c), 11(1)(2).

51 US UETA, s 10.

currently being considered by UNCITRAL in the proposed UNCITRAL Electronic Contracting Convention.[52] As currently phrased, the transaction can only be reversed if the purchaser has not used or received any material benefit or value from the supplied goods or services,[53] although there is no reason why the parties may not agree in advance to a depreciation or "restocking fee" as reasonable compensation to the vendor for the purchaser's reversal of the transaction.

37 It is seriously doubted if similar remedies should avail a vendor who has mispriced or mislabelled goods for sale on his e-commerce webfront. After all, the vendor should not be provided with a legal incentive to resile from his representations regarding the goods being made available for sale. Notwithstanding the ease of use of price-comparison tools on the Internet to check and compare prices of identical or similar goods, the vendor is in a better position than the purchaser to ascertain the correct price for the offered goods. In any event, a mistaken vendor always has available to him a remedy in the law of contractual mistake to reverse the transaction.[54] And if the purchaser has entered into such a transaction *bona fide* believing it to be binding and enforceable, the only way for the vendor to resile from the transaction is for the court to balance the equities of the transaction.[55]

38 Much of the discussion outlined above is applicable, not just to consumers, but also to businesses as purchasers. There is no reason to believe that the three areas of concern outlined above are of no relevance in business-to-business ('B2B') transactions. But, of course, the bargaining positions of parties to a B2B transaction are more equal. The EU Directives solve this problem by respecting the greater party autonomy in B2B transactions and permitting B2B parties to expressly agree to waive the application of these electronic formalities and electronic mistake e-commerce rules to them.

IV. Privacy and Data Protection

39 The advent of the Internet has brought about much convenience to end users by making goods and services readily accessible online. However, this convenience cuts both ways. It has also become likewise easy and convenient for businesses and vendors to collect information about end users. The rise of the Internet has coincided with the rise in the use of electronic data collection and surveillance tools and have escalated concerns in end users about whether or not they are watched on the Internet, and if so, what information is being collected about them, and how disparate pieces of information are being matched to create a profile of the potential customer. A line has to be drawn between the use of technology to collect information about the different aspects of our lives, with a view to promoting business interests and targeting goods and services at interested customers, and the rights of individuals to regulate the use of technology to record our private activities and use and disseminate that personal information – our data protection rights.

A. Model Data Protection Code for the Private Sector

40 Singapore e-commerce consumers are beginning to become more concerned about their privacy on the Internet. Sector-specific regulations such as the Banking Act regime regarding banking secrecy[56] and Telecommunications Competition Code regarding End User Service Information[57] have been legislated to address concerns in the banking and telecommunications markets. Singapore lacks a general non-sector specific legal regime for dealing with data protection. Instead, the decision was taken to adopt a voluntary data protection code for industry

---

52 UNCITRAL draft Convention on Electronic Contracting (12 July 2005 edition), Article 14.

53 US UETA, s 10; UNCITRAL draft Convention on Electronic Contracting (12 July 2005 edition), Article 14.

54 *Chwee Kin Keong & 5 Ors v Digilandmall.com Pte Ltd* [2005] 1 SLR 502, [2004] SGCA 2.

55 *Id*.

56 Banking Act (Cap 19, 1999 Rev Ed), s 47 and Sixth Schedule.

57 Code of Practice for Competition in the Provision of Telecommunication Services 2005, §3.2.6.

self-regulation. In December 2002, the National Trust Council ("NTC"), an industry-led organization supported by IDA, released the Revised Model Data Protection Code for the Private Sector ("the Code"), and this was followed by the adoption of a similar Data Protection Code for the Public Sector by the government in 2004. It has been almost three years since its inception, and an email inquiry by the authors with the NTC and with CommerceNet, one of the organizations charged with enforcing the Code (an Authorised Code Owner ("ACO")[58]), shows that about 200 to 280 commercial companies have since adopted the Code.[59]

41 However, the authors are disappointed to find that neither NTC nor CommerceNet was able to provide any statistics regarding any complaints brought by consumers against businesses to challenge compliance with the Code. Empirical information regarding the types of complaints and the manner in which they are resolved or otherwise with the businesses concerned would have provided affirmation that the ACOs are exercising their supervisory oversight over businesses and confirmed that they are serious about enforcing the Code against recalcitrant businesses. They would also have enabled policy makers to assess the efficacy of the Code. As it stands, however, this assessment of the Code's efficacy can only be done at a jurisprudential level by comparing it with the EU's Data Protection Directive.[60] The rationale for making this assessment is that the data protection codes or regulations in many countries are inspired by Article 25(1) of the EU Data Protection Directive, which places restrictions on the transfers of personal information to non-EU countries where these countries do not have adequate data protection laws. Where Singapore aspires to be a technology, financial and data processing hub, it would establish policies that would facilitate the exchange of personal information into and out of Singapore, including personal information from EU countries. There is therefore good reason to assess the Code against the EU Data Protection Directive. As the following assessment will show, the results are not very encouraging. And in this Paper, the Code has not even been tested against the more rigorous guidelines set out by the EU Data Protection Working Party.[61]

B. Assessing the Data Protection Code

42 The authors propose to conduct an assessment of the Code from two perspectives. The first examines the scope of the data protection rights afforded to individuals – the "data subjects"[62] – against businesses as the entities which determine the purposes and means of processing the personal data – the "data controllers"[63] – as well as the entities actually processing the personal data – the "processors".[64] The second determines the scope of redress of the data subjects against the data controllers and processors for breaches of these rights.

(1) Scope of Data Protection

43 Under the Directive, there are certain minimum expectations of the data subject as against the data controller and processor. Firstly, personal data must be processed fairly and lawfully, collected for specified, explicit and legitimate purposes and not be further processed in a way incompatible with those purposes, be adequate, relevant and not excessive in relation to the purposes for which they are collected and processed, be accurate and kept up to date, and kept in a form which permits identification of the data subjects for no longer than is necessary for the

---

58 The other ACO is the Consumers' Association of Singapore (CASE) via the CaseTrust scheme.

59 Email from NTC and CommerceNet dated 25 and 27 October 2005 respectively.

60 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L 281/31 [*EU Data Protection Directive*].

61 *See* Vili Lehdonvirta, The European Union Data Protection Directive and the Adequacy of Data Protection in Singapore, [2004] SJLS 29.

62 *EU Data Protection Directive*, Article 2(a).

63 *Id*, Article 2(d).

64 *Id*, Article 2(e).

specified purposes.[65] Such personal data may only be processed if the data subject has given his unambiguous consent, or if the processing is necessary for the performance of a contract with the data subject, or if the data controller has to process the data to comply with a legal obligation, or if processing is necessary for a public interest task or in the exercise of official authority, or for legitimate interests pursued by the controller or by parties to whom the data is disclosed.[66]

44 Next, the data subject has to be provided by the data controller with basic information such as information about the controller's identity and the purpose of the processing for which the data is intended.[67] He also has a right to be further informed about the recipients or categories of recipients of the data, his obligations (if any) to reply to the questions posed by the controller for collecting information about him, and his rights against the controller.[68] Even where personal data is not obtained directly from the data subject but from another source, the data controller must also inform the subject of the above basic information.[69] The individual has to be guaranteed rights of access against the data controller as to any personal data collected, with the controller providing basic information such as whether data relating to him is processed, the purposes of processing, categories of data, recipients or categories of recipient, the data being processed, information relating to the source of information and knowledge of the logic involved in any automated processing of the processed data, *without constraint*.[70] In addition, the individual has to be granted the right to rectify non-compliant data,[71] and the right to have his objections notified to third parties to whom the controller has sent the data for processing or disclosure.[72] These rights are subject only to a narrow list of public policy exceptions, namely for national security, defence, public security, criminal prevention, investigation, detection and prosecution, regulation of professions, state-related economic or financial interests, the discharge of official regulatory functions associated with security, crime and finance.[73] The only non public policy exception where the rights above can be derogated from relate to the protection of the data subject himself, or where the exercise of the rights will derogate from the rights and freedoms of other data subjects.[74]

45 In comparison, the broad principles in the Code found in Principles 2 (Specifying Purpose), 3 (Consent), 4 (Limiting Collection), 5 (Limiting Use, Disclosure and Retention), 6 (Accuracy) and 9 (Individual Access and Correction) translate well into the rules in the EC Data Protection Directive outlined above. A closer examination of the provisions in the Code will show up some derogations from the EU provisions. For instance, the EU Data Protection Directive requires that personal data be collected, processed and used "for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes".[75] Clause 4.2 of the Code acknowledges the same principle of "specifying purpose", and goes on to state, sagely that:

> The difficulty of developing new uses of data beyond those identified in the very beginning can be overcome by an organization having a clear vision and far-sighted business plans.

---

65 *Id*, Article 6.

66 *Id*, Article 7.

67 *Id*, Article 10.

68 *Id*.

69 *Id*, Article 11. This is subject only to the exception where the information is processed for statistical purposes, or for historical or scientific research, whereupon it becomes impossible or disproportionately difficult for such information to be supplied to the data subject. *Id*, Article 11(2).

70 *Data Protection Directive*, Article 12(1).

71 *Id*, Article 12(2).

72 *Id*, Article 12(3).

73 *Id*, Article 13(1).

74 *Id*, Article 13(1)(g).

75 *Id*, Article 6(1)(b).

46 Yet clauses 4.2.4, 4.3, 4.4 and 4.5 of the Code go on to prescribe ways in which personal data that is collected may be used for a purpose not previously specified ("the new purpose shall be specified to the relevant party prior to use"[76]), or collected, used or disclosed beyond specified purposes where one of the following conditions is satisfied:

(a) Collection/use is consented to by the individual;[77]

(b) Collection/use/disclosure is clearly in the interests of the individual, it is impractical to obtain the consent of the individual and if it were practical to obtain such consent, the individual would likely give it;[78]

(c) [Collection/use with the knowledge or consent of the individual would compromise the availability or accuracy of the data] where such collection/use/disclosure [pertains to/is reasonable for purposes related to] an investigation of an actual or suspected breach of an agreement or contravention of the law that has been, is being, or is about to be committed;[79]

(d) Data is being collected/used/disclosed in an emergency that threatens the life, health or security of a person;[80]

(e) Collection/use is data which is generally available to the public [in that form];[81]

(f) Disclosure is made to a solicitor representing the organization [data controller];[82]

(g) Disclosure is necessary for the purposes of establishing, exercising or defending legal rights;[83]

(h) Disclosure is to a government agency that has made a lawful request for the data;[84]

(i) Disclosure is made to an institution whose purpose is the conservation of records of historic or archival importance and disclosure is for such purpose;[85] and

(j) Disclosure is made, on the initiative of the organization [data controller], to an investigative body appointed by the organization, or to a government agency, for investigative purposes.[86]

47 "Consent" is generally a panacea for data collection and processing that exceeds the original purpose for which data was collected and processed. "Consent" that is required in the EC Directive has to be "unambiguous"[87] and "explicit"[88]. However, the collection and processing of data may exceed the purposes expressly consented to by the data subject. Where the exceptions

---

76 Model Data Protection Code, clauses 4.2.4, 4.3.1.

77 *Id*, clauses 4.2.4, 4.4(e), 4.5(e).

78 *Id*, clauses 4.3(a), 4.4(a), 4.3(e), 4.3(i), 4.5(a), 4.5(f).

79 *Id*, clauses 4.3(b), 4.3(f), 4.4(b), 4.3(p), 4.5(b), 4.5(n).

80 *Id*, clauses 4.3(c), 4.3(g), 4.4(d), 4.3(m), 4.5(c), 4.5(k).

81 *Id*, clauses 4.3(d), 4.3(h), 4.4(d), 4.3(o), 4.5(d), 4.5(m).

82 *Id*, clause 4.3(j), clause 4.5(g).

83 *Id* clause 4.3(k), clause 4.5(h).

84 *Id* clause 4.3(l), clause 4.5(i).

85 *Id* clause 4.3(n), 4.5(l).

86 *Id*, clause 4.5(j).

87 *Data Protection Directive*, Articles 7(a), 26(1).

88 *Id*, Article 8(2)(a).

pertain to protecting or serving the interests of the data subject, such as (b) and (d) (described in the EC Directive as "necessary in order to protect the vital interests of the data subject"[89]), there is little objection in conjunction with such purposes. Likewise, where the exceptions pertain to the data controller's legal obligations[90] or where this is required in the public interest or exercise of official duty vested in the controller or in a third party to whom the data is disclosed,[91] such as (h) and (i) (assuming that the institution is a government institution such as the National Archives), there is again little objection. It would seem that exceptions (c) and (j) were drafted with this public interest exception in mind, except that they are ambiguous and unnecessarily wider than the public interest objective. For instance, it is a bit presumptuous to assume that a data subject's rights can be disregarded when the data controller suspects that a breach of law is about to be committed. Which law empowers a data controller to conduct criminal investigations against its data subject? And will the data subject have any rights of redress against a data controller should such investigations turn out to be unnecessary or unwarranted? Similarly, why should a data controller resile from its data protection obligations simply because it appoints an internal body as an "investigative body" to conduct investigations in exception (j)? If these are legitimate police investigations or investigations by a government agency, they can clearly be brought under exception (h).

48 The presence of the other exceptions is hardly conducive to the confidence of the data subject, despite knowing that the Code states that "knowledge and consent of the individual are required for the collection, use or disclosure of the personal data to a third party". It is not easy to justify the other non-consented purposes, particularly since they seem to have little bearing on the interest of the data subject. For instance, exception (b) claims that collection, use or disclosure for a non-consented purpose may be pursued, where it is "clearly in the interests of the individual". And it is somewhat presumptuous to believe that it would be impractical to obtain the consent of the individual and that if it were practical, the individual would likely give it. If the rubric of this exception is "implied consent", it could be reworded as one which sanctions the processing of the collected data that is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject entering into a contract.[92] Similarly, an exception entitling the data controller's disclosure "for the purposes of establishing, exercising or defending legal rights" does not indicate whose rights the disclosure is for – the data subject's, the data controller's, or a third party's. There is no nexus between the Code-approved disclosure and the data subject in exceptions (e), (f) and (g). It would seem that these exceptions are inserted purely for the benefit of the data controller with disregard for the interests of the data subject.

49 On balance, while the Code seeks to capture the spirit of protecting the data subject's rights in his personal data, the exceptions that are recognized severely derogate from this spirit. It could hardly be said that a data subject in Singapore has a high quality data protection right under the Code, when comparing his rights with his counterparts in Europe and many other countries with data protection laws that are based on the EC Data Protection Directive.

(2) Enforcing the Rights of the Individual

50 One of the common criticisms levelled against the Code is that it is a voluntary industry regulatory code, as opposed to legislation to enforce the individual's data protection rights. However, this criticism is too broad, as the US Department of Commerce's Safe Harbour Privacy Principles is also a voluntary industry regulatory code which has been approved by the European Commission as being adequate under Article 25(6) of the EC Data Protection Directive.[93] The relevant test is the efficacy of the rights of redress of the data subject against the data controller

---

89 *Id*, Article 7(d).

90 *Id*, Article 7(c).

91 *Id*, Article 7(e).

92 *Id*, Article 7(b).

93 US Department of Commerce, *Introduction to the Safe Harbour*, at http://www.export.gov/safeharbor (accessed 23 December 2005).

and the processor.[94] This right of redress has to come with "teeth". EC Data Protection Directive states that if a data controller fails to respect the rights of data subjects, national legislation must provide for a judicial remedy whereby the controller must compensate a person who has suffered as a result of any unlawful processing in damages.[95] In addition, the Directive recognizes that the establishment of supervisory authorities, exercising their functions with complete independence, must have the necessary means to perform their supervisory duties over the data controllers, including powers of investigation and intervention, particularly in the case of complaints from data subjects, and powers to engage in legal proceedings.[96]

51 Herein lies the biggest shortcoming of the Model Data Protection Code. The Code is business-centric: it directs a series of obligations at businesses and organizations in their capacities as data controllers.[97] It does not engage third parties as independent bodies. Thus while it is appropriate for businesses to put in place a redress mechanism, the ACO has to put in place an internal dispute resolution mechanism for handling disputes between TrustSg accredited companies and their customers. The correspondence from CommerceNet as an ACO states:

> Basically for CommerceNet Singapore, all accredited companies are briefed on our Dispute Resolution Mechanism. CommerceNet Singapore as an ACO has in place a 3-Step Internal Dispute Resolution Mechanism for handling disputes that arise between TrustSg accredited companies and their customers, they [sic] are:
>
> (i) Direct Negotiation
>
> (ii) Recommendation for Settlement
>
> (iii) Mediation
>
> In the event that the ACO fails to resolve the disputes satisfactorily, we would direct and advise the parties concerned to access an independent Alternative Dispute Resolution (ADR) scheme such as the Singapore Mediation Centre or the Small Claims Tribunal. So far we have not received any complaints on data protection disputes from consumers or corporate companies about our accredited companies. CommerceNet Singapore would terminate the membership of an accredited company if they breach the code of practice.

52 This, it is submitted, falls far short of the requirements of the EC Directive. Firstly, the nature of the current judicial remedy available to an aggrieved data subject is probably contractual, and only as against the business as the data controller, for failing to observe its obligations under the Code.[98] Next, there is hardly any available publicly available documentation [to verify] regarding the role and responsibility of the ACO as against the data controller as a TrustSg accredited company, particularly as regards its investigation and intervention responsibilities, such as to order the data controller to block, erase or destroy the relevant data, or impose a temporary or definitive ban on processing, or warning or admonishing the data controller.[99] Even if such documentation exists and is publicly available, the data subject can only pursue his redress against the ACO in the tort of misrepresentation. There is no mention of any compensation to the data subject for the harm he has suffered, let alone any attempt at quantification. Likewise, a claim that "in the event that the ACO fails to resolve the dispute satisfactorily, we would direct and advise the parties concerned to access an independent Alternative Dispute Resolution scheme" is an attempt at disengaging itself from the data subject's exercise of his rights, administratively and

---

94 *Data Protection Directive*, Article 2(e).

95 *Id*, Recital (54), Articles 22-24.

96 *Id*, Recital (62), Article 28.

97 Model Data Protection Code, para 3.3.

98 Under Singapore law as it stands, there is no express recognition of a privacy right. It has been contended that the common law provides sufficient privacy or data protection rights such as the obligation of confidence in *Douglas and Others v Hello! Ltd and Others (No 3)* [2003] All ER 996 but that case is explicable on the peculiar circumstances in which the Douglases sought to commercialise their wedding event. The case of *Malcomson Nicholas Hugh Bertram & Anor v Naresh Kumar Mehta* [2001] 4 SLR 454 is likewise limited in its application, as not all data collection, use and processing activities will amount to the tort of harassment.

99 *Data Protection Directive*, Article 28(3). A reference to the right of the ACO to terminate the membership of an accredited data controller is hardly assuring to the aggrieved data subject. Likewise, the data controller is entitled to a fair measure of the transparency in the manner in which the ACO reaches its decision to terminate the TrustSg accreditation of the data subject.

substantively. Presumably, at this stage, the data subject would have rejected the data controller's attempts at settlement and mediation attempts, and is insisting on his strict legal rights. The least the ACO could do is to make a ruling, after hearing the data subject's claims and conducting an investigation, as to whether or not there is evidence to substantiate the data subject's claim or to accept the data controller's excuse, if any, for breach of the Code.[100]

53 As the supervisory authority, the ACO should also conduct its activities in a transparent and accountable manner, and make publicly available its reports at regular intervals.[101] This will raise the profile of the ACO as well as its standing with businesses seeking accreditation as well as with discerning data subjects, and add to the value of the TrustSg mark.

C. Government Data Protection Laws

54 There are many statutes that govern various public sector uses of personal data. These include the Official Secrets Act[102], the Statistics Act[103] and the Central Provident Fund Act[104]. These statutes typically regulate and criminalize the unauthorized release of personal information which government agencies collect about citizens and residents. But they do not prescribe the rights of individuals to regulate the collection, use and dissemination of personal information by government agencies. In fact, some [agencies] have exercised the prescriptive power in the Statistics Act to *require* individuals to supply personal information, under the reason of statistics collection, with the threat of criminal sanction for any refusal to do so. This has given rise to some grouses being directed at the agencies concerned, particularly where the agency seeks to collect personal information from an EU foreigner residing in Singapore.

55 It could have been assumed that the Singapore Government Public Sector Data Protection Policy would clarify the rights of citizens and residents as regards the collection, use and dissemination of personal information. It is widely believed that the Government Public Sector Data Protection Policy is modelled on the Private Sector Data Protection Code. However, the Government appears to have chosen to treat its own Public Sector Policy as secret since it is not in the public domain, other than as translated in terms found at the websites of individual government departments and bodies. Notably, there is no means for a citizen or resident to check these published website terms for consistency and compliance with the Public Sector Policy. This move appears paradoxical, particularly since one of the cardinal principles behind a Data Protection Code is transparency and openness. If the Government does not make readily available information about its own Data Protection policies and procedures for handling personal data, there would be no "rights" as such that a citizen or resident can avail himself of in relation to the protection of his data in his dealings with the Government.

56 Of course, the above review about Singapore's data protection laws may seem particularly biased, since the assessment is made with one of the most comprehensive and well-thought out data protection schemes in the world – the EC Data Protection Directive. But it is submitted that this review is necessary, particularly since many countries are upgrading their data protection laws to bring them in line with the EC Data Protection Directive. And a strengthened data protection regime will bring benefits, not only for individuals and consumers in the electronic environment, but also bring economic benefits for Singapore vendors that are engaged in the global data processing network. For this reason alone, we should bring our data protection laws in line with the EC Data Protection Directive as soon as possible.

---

100 *Id*, Article 28(4).

101 *Id*, Article 28(5).

102 Cap 213, 1985 Rev Ed.

103 Cap 317, 1999 Rev Ed.

104 Cap 36, 2001 Rev Ed.

V. Electronic Money

57 To the extent that Singapore aspires to be a hub for electronic commerce, the laws surrounding the establishment and operation of payment systems that facilitate the use of electronic money ("e-money") take on heightened significance. Even as the success of the Singapore Government's campaign for a "cashless society"[105] is borne out by the widespread use of Automated Teller Machines ("ATMs"), Electronic Funds Transfer at Point of Sale ("EFTPOS") and Interbank GIRO for making payments in Singapore, the regulation of e-money remains a thorn in the side of IT law development.

58 E-money is premised on its multi-purpose facility which is good for use with a number of vendors. Its increasing acceptance and popularity in Singapore are illustrated by the growing use of the NETS CashCard in payments for Electronic Road Pricing (ERP) dues and car park charges and the ez-link card for fare on Singapore's public transport system (and more and more in other retail sectors such as payment at food and beverage outlets, convenience stores and self-service kiosks).[106] According to the 2004/2005 Annual Report of the Monetary Authority of Singapore ("MAS"), the value of payments by multi-purpose stored value facilities rose by 7% to S$1.3 billion.[107]

59 Despite such increased numbers, the effective confinement of e-money systems in Singapore to the NETS CashCard and the ez-link card to-date is attributable to the prevailing (but expected to be soon outdated) section 77A of the Banking Act [108] which prohibits the issuance of any stored value card other than by a bank with the approval of MAS or otherwise for payment only of goods and/or services provided by the issuer. The wide definition of "stored value card"[109] has arguably had a chilling effect on more than a couple of proposed online payment systems on which one of the authors has advised and which were thereby prevented from being launched.

60 While these remain unavailable for discussion due to reasons of professional confidence, the much publicized case involving the high-profile Indigoz Exchange Pte Ltd in early 2005 is sufficient illustration of section 77A thwarting innovation. In that case, the company's issuance of dining vouchers called "i-chqs" that could be used at about 260 restaurants, led the Commercial Affairs Department to commence investigations against the company and make a finding that it had thereby breached section 77A, and MAS to impose a fine on the company for the contravention.

61 The well-meaning intent of section 77A to protect users of multi-purpose stored value cards ("MPSVCs") is obvious. It limits issuers of MPSVCs to licensed banks which are obliged to maintain such reserve and liquidity requirements as MAS may determine in relation to the proceeds arising from every issue of any MPSVC and to comply with such terms and conditions under which the MPSVC may be issued, as determined by MAS.[110]

62 Online payment systems set up and operated by non-bank entities, involving the use of a credit facility for which payment is made in advance and which is available, up to the amount of that facility, for online shopping activities, are easily conceivable. However, section 77A limits

---

105 Charles Lim Aeng Cheng, *"The UNCITRAL Model Law on International Credit Funds Transfers"* (1993) SJLS 538.

106 Monetary Authority of Singapore Annual Report 2004/2005 at 45.

107 *Id*, at 44.

108 Cap 19, 2003 Rev Ed.

109 Defined in the Banking Act, section 77A(9) to mean "a card for which a person pays in advance a sum of money to the issuer in exchange for an undertaking by the issuer that on the production of the card to the issuer or a third party (whether or not some other action is also required), the issuer or the third party, as the case may be, will supply goods or services or both goods and services" and to include "any token, coupon, stamp, form, booklet or other document or thing".

110 Banking Act, section 77A(2) and (3).

the setting up of such payment systems and facilities, which can serve to facilitate e-commerce. In April 2003, MAS issued its first public consultation paper on the proposed enactment of a Payment Systems Oversight Act.[111] This was followed by its further consultation paper in December 2004.[112] Following feedback on these consultation papers, the draft Payment Systems (Oversight) Bill ("Bill") was consequently introduced for first reading in Parliament on 21 November 2005.[113]

63 The Bill seeks to provide a uniform basis for MAS to oversee payment systems and stored value facilities[114] in Singapore and adopts a risk-based approach to such oversight, in recognition of the varying risk profiles of different payment systems *inter se* and *vis-à-vis* stored value facilities. In particular, the focus will be on "payment systems that are considered important in terms of stability of the financial system and public confidence"[115] and only designated payment systems which meet these criteria will be regulated. All other payment systems and likewise, stored value facilities, will only be subject to the information gathering powers of MAS.[116]

64 Under this scheme, an MPSVC is considered a "stored value facility" ("SVF") which is defined[117] as:

> "(a) a facility (other than cash), whether in physical or electronic form, which is purchased or otherwise acquired by a person (referred to in this Act as the user) to be used as a means of making payment for goods or services up to the amount of the stored value that is available for use under the terms and conditions applying to the facility, and payment for the goods or services is made by the holder of the stored value in respect of the facility (rather than by the user); or
>
> (b) all the facilities referred to in paragraph (a) provided under the same terms and conditions".

No distinction is made between a single purpose SVF ("SPSVF") and a multi-purpose SVF ("MPSVF")[118] and indeed these expressions are not featured anywhere in the Bill. Instead, the line between generally permissible SVFs and restricted SVFs is drawn on the basis of a prescribed amount of the aggregate "stored value" which is defined[119] as:

> "the sum of money that –
>
> (a) has been paid in advance for goods or services intended to be purchased through the use of the stored value facility;
>
> (b) is available for use from time to time for making payment under the terms and conditions applying to the stored value facility; and

---

111 Monetary Authority of Singapore Consultation Paper, *Payment Systems Oversight Act* (April 2003), at http://www.mas.gov.sg/resource/download/MASConsultationPaperonPaymentSystemsOversightAct.pdf (accessed 27 December 2005).

112 Monetary Authority of Singapore Consultation Paper on *Draft Payment Systems (Oversight) Bill*, December 2004, at http://www.mas.gov.sg/masmcm/upload/mm/MM_FECD1D20_6295_5312_4E08C3EAD82FEA59__FECD1D30_6295_5312_40256068939CBE3D/Consultation%20Paper%20on%20Draft%20Payment%20Systems%20(Oversight)%20Bill.pdf (accessed 27 December 2005).

113 The Payment Systems (Oversight) Bill (No. 39/2005) addressed some of the public feedback given to the earlier draft version of the Bill annexed to the *Payment Systems Oversight Consultation Paper*.

114 The use of the expression "facilities" in substitution for "card" was adopted by MAS to "reflect the technology neutral stance of MAS' policy in this area" and in recognition of "technological advancements and innovations … in different forms of stored value solutions". *See, supra* n 111, at 25.

115 *Id*, at 2.

116 Payment Systems (Oversight) Bill, sections 6 and 29.

117 *Id*, section 2.

118 The expression "MPSVF" is used (and distinguished from a single purpose stored value facility or "SPSVF") in MAS' Consultation Paper on *Draft Payment Systems (Oversight) Bill*, December 2004, *supra* n 112, at 5-6 and also in MAS, *Response to Feedback Received – Consultation on Draft Payment Systems Oversight Bill* at http://www.mas.gov.sg/masmcm/bin/pt1Response2feedback_on_Draft_Payment_Systems_Oversight_Bill.htm (accessed 23 December 2005) at para 6-11.

119 Payment Systems (Oversight) Bill, section 2.

(c) is held by the holder of the stored value facility".

Specifically, any non-bank entity is permitted to issue a SVF as long as the aggregate stored value (or float) remains within the statutorily prescribed cap, presently set at S$30 million. Any SVF which exceeds the prescribed amount may only be issued as a widely accepted ("WA") SVF[120] by an MAS approved holder with the backing of an MAS approved bank,[121] as distinguished from a non-widely accepted ("NWA") SVF.[122] The Bill accordingly repeals section 77A of the Banking Act.[123]

65 According to MAS, the proposed distinction between NWA SVFs within the $30 million limit and WA SVFs that exceed the limit, operates on the bases that the prescribed amount is a "proxy indicator for how widely used and accepted"[124] an SVF is and that some SVFs may have a "lower level of funds-at-risk"[125] than those which are more widely accepted. By avoiding the issue that has been the apparent concern of section 77A *i.e.* the unregulated taking of monetary deposits by non-banks for use as *de facto* cash (no matter what the amount is), the Bill seems to have swung the pendulum in the other direction.

66 Among the attractions of e-commerce are the consumer's convenience and power of choice, including the ability to pay for small purchases such as downloaded music or electronic literature, using SVFs or e-money without the need to deal with physical change nor the need for a credit card or debit card. To be able to do so in an environment where consumers know that the people who are legally permitted to establish systems which involve taking their money in advance, are subject to at least basic obligations with respect to such money, must surely go a long way towards bolstering confidence in the legitimacy and propriety of these systems that facilitate such convenience and hence encourage their use.

67 In this regard, it is hard to say whether the liberalization of SVFs in the manner proposed under the Bill where there is no regulatory obligation on the part of issuers and holders of NWA SVFs to protect the float, will pave the way for the growth of legitimate payment systems involving the issuance and use of e-money. Indeed the success of the NETS CashCard and the ez-link card may well be attributable to consumer confidence arising from the protective effect of section 77A.

68 In the wide space between the restrictions of section 77A (where enterprise and innovation in the development of e-money systems are left cold and the Indigozes of Singapore are compelled to abandon their activities) and the proposed almost free-for-all approach of the Bill (where consumers of niche businesses are left to fend for themselves or to otherwise deal only with the big boys of WA SVFs), lies a possible turf of measured regulation that could be parleyed to preserve both innovation of e-money systems and consumer confidence in them. The theme of such regulation would be that the float is not money which belongs to those who hold it and must therefore be accounted for, whether or not going so far as constituting a trust in favour of the consumers who place the money in the float. Hence, if confidence in e-money systems is to be ensured, the law could do more, such as to require the holder of an SVF to maintain liquidity in a minimum amount of the float under a separate account and to prevent it from charging such account in favour of any creditor or lender and in the event of the holder's bankruptcy or

---

120 *Id.*, section 33.

121 *See* definition of "widely accepted stored value facility" in section 2(1) of the Payment Systems (Oversight) Bill, which requires an approved bank to be fully liable for the stored value of a widely accepted stored value facility. *See also* definitions of "approved holder" and "approved bank" in section 2(1).

122 *See* Consultation Paper on *Draft Payment Systems (Oversight) Bill*, *supra* n 112 at 5 where the expression"non-widely accepted MPSVF" is used.

123 Payment Systems (Oversight) Bill, section 58.

124 Consultation Paper on *Draft Payment Systems (Oversight) Bill*, *supra* n 112, at 5.

125 *Id.*

liquidation, to provide that payment of the proceeds from such account must be made to the users in priority to other creditors.

69 Clearly the Bill has not been developed in the absence of any consideration for consumer protection.[126] The eventual rejection of any consumer protection measures other than reserving the possibility of regulations that require holders[127] of SVFs to mark or label their SVFs,[128] seems to have been the result of a balancing act between favouring the benefits of such measures and avoiding the increased costs to and regulatory burden on NWA MPSVFs.[129] Such *caveat emptor* approach overly presumes the ability of consumers to assess and manage their own risk of whether to buy into any particular MPSVF, bearing in mind that consumers are typically already challenged by having to navigate their way through the myriad complex terms and conditions, including, for instance, those that provide for an expiry date on the credit in their SVFs, or limit the types of purchases possible with their SVFs, or even reverse the burden on the consumer to prove that he has credit on his SVF with the SVF holder. Considering certain European benchmarks for regulatory safeguard of electronic money which address for example, issues of redemption of e-money at par upon request, the possibility of imposing reserve requirements, security against counterfeits, full investment backing in eligible assets, minimum validity period of e-money issued, limits on the value of e-money issued per purse and other consumer protection measures,[130] the Bill as it stands falls short.

70 Of course, we make these comments without the benefit of examining the Regulations which will be issued pursuant to the Bill for the regulation of SVFs. How this will pan out in the hope that innovative e-money systems will thrive to take e-commerce to the next level is anybody's guess. It is conceivable that the course to be developed in this quest as determined by the degree of public confidence in these systems might not be as dependent on the formulation of consumer protective law as on the general integrity of the players in the NWA SVF game in Singapore, in which case the *caveat emptor* approach might well be the right one to make. However, as the Bill effectively enables non-bank entities to legally hold funds practically as banks do but without the corresponding checks attendant on banks, the need to legislate on consumer protection in the world of MPSVFs is more, and not less, important than with banks.

VI. Domain Names

71 As the registration authority for country code top level domain ("ccTLD") names in Singapore ending with ".sg", Singapore Network Information Centre Private Limited ("SGNIC") adopted the Singapore Domain Name Dispute Resolution Policy ("SDRP") with effect from 15 November 2001 as the framework and mechanism for the resolution of disputes relating to Singapore ccTLDs to "offer a quicker and cheaper way … compared to litigation in the courts."[131] Since its adoption, the SDRP has been applied to resolve four Singapore ccTLD disputes in 2002, which was followed by a period of inactivity until 2005 when five disputes were submitted for resolution through the SDRP.

---

126 *See* MAS, *Response to Feedback Received – Consultation on Draft Payment Systems Oversight Bill*, *supra* n 118, at para. 9.2.

127 A "holder" is defined in the Payment Systems (Oversight) Bill, section 2 as the person who holds the stored value and makes payment for goods or services referred to in the definition of "stored value facility".

128 *Id.*, section 30. It might well be, as indicated by MAS in its *Response to Feedback Received – Consultation on Draft Payment Systems Oversight Bill*, *supra* n 118, at para 9.2 that holders of NWA MPSVFs would be required pursuant to regulations to put up notices stating that their NWA MPSVFs are not subject to MAS approval.

129 *See* MAS, *Response to Feedback Received – Consultation on Draft Payment Systems Oversight Bill*, *supra* n 118, at para 9.2.

130 *See* European Central Bank, *Report on Electronic Money (1988)* and UK Financial Services Authority, *Policy Statement (2002).*

131 *See* http://www.disputemanager.com.sg/sdrp/what.asp (accessed 29 December 2005).

72 The authors propose to take stock of how the SDRP has fared since its adoption, particularly with reference to the application of the Uniform Domain Name Dispute Resolution Policy ("UDRP") established and adopted with effect from 24 October 1999 by the Internet Corporation for Assigned Names and Numbers ("ICANN") for both generic top level domain ("gTLD") names e.g. ending with ".com", ".net" and ".org" and certain ccTLD names, after which the SDRP is fashioned.

A. UDRP vs. SDRP Provisions

73 Both the UDRP and SDRP operate on the basis of the underlying contractual rights and obligations binding the registrar who issues the domain name in question and the holder or registrant to whom (and indeed on the basis of which rights and obligations) the domain name is issued. In particular, the registrar reserves the contractual right to withdraw the assigned domain name from the registrant pursuant to a finding to this effect under the proceedings of the UDRP or SDRP proceedings.

74 Under the UDRP provisions, a complainant would succeed in having a domain name cancelled or transferred to the complainant if it proves that:

(a) the registrant's domain name is identical or confusingly similar to a trade mark or service mark in which the complainant has rights; and

(b) the registrant has no rights or legitimate interests in respect of the domain name; and

(c) the registrant's domain name has been registered and is being used in bad faith.

75 The corresponding SDRP provisions differ from the above UDRP provisions only in the following two apparently minor but potentially significant respects:

(a) under the first condition, the complaint may be based not only on the domain name being identical or confusingly similar to the complainant's trade mark or service mark but also to the complainant's *name*; and

(b) under the third condition, the complainant need only prove that the domain name has been registered *or* is being used in bad faith, and not both registration and use in bad faith.

76 Simply from the difference in wording, the SDRP provisions come across as more liberal in favour of complainants but is this is borne out by the cases applying the different wording?

B. Statistical Comparison

77 The World Intellectual Property Organisation ("WIPO") reports the following numbers on cases decided under the UDRP provisions which ruled in favour of the complainant (disregarding those that were cancelled, withdrawn or terminated after submission):[132]

(a) 5084 (approximately 84%) out of 6075 decided cases on gTLDs; and

(b) 162 (approximately 85%) out of 191 decided cases on ccTLDs.

78 In comparison, four (exactly 50%) of the eight decided cases under the SDRP provisions (one having been settled) resulted in the transfer of the domain name in favour of the

[132] Results as of 18 December 2005 posted at http://arbiter.wipo.int/domains/statistics/cumultaive/results.html (accessed 29 December 2005).

complainant.[133] Although the statistically insignificant sample size of cases decided under the SDRP provisions may prevent us from drawing any real conclusions, it may perhaps be observed that the more liberal language of the SDRP provisions has not resulted statistically in any greater proportion of decided cases that ruled in favour of the complainant than has been done with the UDRP cases.

C. Complainant's Rights

79 Given that a complaint under the SDRP provisions may also be founded on the complainant's rights in a name *per se* (and not just on trade mark or service mark rights as required under the UDRP provisions), to what extent have the SDRP decisions turned on this additional ground?

80 Despite the availability of the complainant's rights in a name as a basis for proceeding under the SDRP, the analyses in all the SDRP cases revolved around the complainant establishing rights in a trade mark sense. Indeed, all the complainants in the four cases which found in their favour[134] owned trade mark registrations which went towards the Panels' findings that they had the requisite "rights" to succeed under the SDRP proceedings. Although the Panel in two of the remaining four SDRP cases which found for the respondent[135] omitted its express analysis for the finding that the complainant had the necessary rights, it is notable that the complainant in those cases also owned trade mark registrations which one assumes formed the basis for the Panel's finding that the complainant's rights had been established (notwithstanding the eventual failure of the complainant's action due to its inability to prove the remaining conditions required under the SDRP provisions).

81 Interestingly, in the remaining two cases which favoured the respondent, the Panel's determination of whether the complainant possessed the requisite "rights" was undertaken on the basis of requiring the additional element of exclusivity in those rights. In the first of these cases, the *MTV Case*, to the extent that the complainant was unable to establish that it had acquired exclusive rights over the word "mtv" (despite its registrations of certain "mtv" & logo trade marks overseas), especially in the light of the finding by the Panel that the word "mtv" (but not the "mtv" trade mark) had become genericised in the Chinese music industry,[136] the Panel was not prepared to recognize that the complainant had the necessary rights such as to displace the respondent, and took a heavily trade mark-oriented approach to determining the establishment of the complainant's rights. Similarly in the second of these cases, the *Teletext Case*, the Panel broached the matter of the complainant's "rights" from the trade mark perspective, stating that these rights "are readily demonstrated if the name or mark is a registered trade mark under the Trade Marks Act … [or] under the law relating to passing off" and also found for the respondent because the complainant failed to establish that the word "teletext" had come to be distinctive of the complainant's services.[137]

82 It does not appear that a complainant under SDRP proceedings has effectively any more leeway than a complainant under UDRP proceedings in respect of the first condition required to be established, notwithstanding the additional reference in the SDRP provisions to a "name" over

---

133 Results posted at http://www.disputemanager.com.sg/sdrp/Proceedings_info.asp (accessed 29 December 2005).

134 *Google, Inc v Googles Entertainment*, SDRP Case No. 2002/0003(F); *Samsung Electronics Co., Ltd v Funexpress.com.sg Pte Ltd*, SDRP Case No. 2002-0004(F); *McDonald's Corporation v Naturerise, Inc*, SDRP Case No. 2005/0001(F); and *Linguaphone Institute Limited and Linguaphone Singapore Pte Ltd v Cambridge Information Technology and Chan Ngah Kok*, SDRP Case No. 2005/0002(F) [*Linguaphone Case*].

135 *Teck Leong Metals Pte Ltd v Ban Soon Cheong Pte Ltd*, SDRP Case No. 2005/0004(L); and *Teck Leong Metals Pte Ltd v Teck Leong Industries Pte Ltd*, SDRP Case No. 2005/0005(L).

136 *Viacom International Inc. v Elite Technologies Co Ltd*, SDRP Case No. 2002/0001(F) at para 6.2.3 and para 6.2.7 [*MTV Case*].

137 *MediaCorp News Pte Ltd v iLABS Technologies*, SDRP Case No. 2002/0002(L) at para 6.9 [*Teletext Case*].

which the complainant has rights and with which the domain name in dispute is identical or confusingly similar. If the apparently deliberate addition of the word "name" in the SDRP provisions (which is absent from the UDRP provisions) was intended to assist a complainant with rights in a name such as a business or company name but no trade mark rights, the current direction of the decided SDRP cases have not made this clear. However, the reality is that none of the complainants in the decided SDRP cases founded his claim on rights to a "name" *per se*.

83 The strong focus on trade mark-related considerations in the SDRP cases have effectively equalised the practical application of the SDRP provisions with the UDRP provisions in relation to the first condition required to be established by the complainant, despite the difference in language that might have looked at first sight to make a potentially significant difference in an appropriate case. For example, the consensus view of the WIPO Panels in the UDRP cases, as examined in the WIPO Overview of WIPO Panel Views, is that if the complainant owns a registered trade mark, he will have satisfied the first element of the UDRP provisions[138] seems equally prevalent among the Panels in the SDRP cases.

D. Respondent's Rights or Legitimate Interests

84 While the language in the UDRP and SDRP provisions on the second element required to be proved by a complainant is the same, *i.e.* the registrant has no rights or legitimate interests in respect of the domain name, there appears to be more clarity on this issue under the UDRP cases that once the complainant has made out its *prima facie* case that the respondent lacks rights or legitimate interests in the mark, the burden of proving the respondent's rights or legitimate interests shifts to the respondent, failing which the complainant would be deemed to have proved the lack of such rights or interests.[139]

85 The singular message coming out of the SDRP decided cases on this issue is less clear and perhaps because the collection of such cases is presently small, the verdict is still open. While several of the Panels in the SDRP cases either expressly or obliquely assumed the consensus UDRP position that the burden of proving the respondent's rights or interests in the domain name falls on the respondent if the complainant's assertion of the lack thereof is to be rebutted, the Panels in at least a couple of the SDRP cases did not necessarily agree with this.[140]

85 The WIPO UDRP cases are equally clear in the contention that the respondent's right or legitimate interest in the domain name is not proved merely by the domain name comprising a generic word.[141] For example, in the UDRP *Madonna Case*,[142] the fact that the word "Madonna" had an ordinary dictionary meaning that was not associated with the complainant was given little weight. Notably, the WIPO Overview of WIPO Panel Views also states that if a respondent is using a generic word to describe his product or business, it has a legitimate interest in the domain name.[143]

86 In the three SDRP cases where the domain name in question was argued by the respondent to be a generic word, the Panel in the:

---

138 *See* WIPO, WIPO Overview of WIPO Panel Views on Selected UDRP Questions, at para 1.1 at http://arbiter.wipo.int/domains/search/overview/index.html (accessed 23 December 2005).

139 *Id.*, at para 2.1.

140 *See, e.g., Linguaphone Case, supra* n 134, where the Panel's position on the issue of who has the final burden of proving the lack of the respondent's rights or interests in the domain name is not entirely clear. *See also MTV Case, supra* n 136, at paras 6.3.4 and 6.3.6.

141 WIPO, WIPO Overview of WIPO Panel Views on Selected UDRP Questions *supra* n 138, at para 2.2.

142 *Madonna Ciccone p/k/a Madonna v Dan Parisi and "Madonna.com"*, WIPO Case No. D2000-0847.

143 WIPO, WIPO Overview of WIPO Panel Views on Selected UDRP Questions *supra* n 138, at para 2.2.

(a) *MTV Case* relied on this as a basis for its finding that the complainant had therefore failed to prove the respondent's lack of rights or legitimate interests in the domain name;[144]

(b) *Teletext Case* did not expressly consider this in the context of its determination of whether the respondent had rights or legitimate interests in the domain name;[145] and

(c) *Linguaphone Case* rejected this altogether as a relevant argument in the proceedings.[146]

87 The generally more disparate outcome of the SDRP decided cases may well be attributable not only to the facts that the SDRP regime was only implemented in 2001 and the domain name market in Singapore is still evolving, but also to the fact that most of the SDRP decided cases involved relatively complex factual dynamics as compared to the good number of the more straightforward cyber-squatting type cases among the UDRP cases.

E. Respondent's Bad Faith

88 In the UDRP language on the third condition to be proved by a complainant, the "significance of the use of the conjunction "and" is that paragraph 4(a)(iii) requires the Complainant to prove use in bad faith as well as registration in bad faith. That is to say, bad faith registration alone is an insufficient ground for obtaining a remedy".[147] Hence in the *Famosa Case*,[148] the UDRP Panel declined "to state a formal finding as to whether the Respondent is using the domain name in bad faith, because the failure to prove bad faith registration is dispositive". Similarly, in view of the complainant's permission for the respondent's original registration of the domain name, the UDRP Panel in the *Greentyre Case*,[149] found that such registration was in good faith and stated in the circumstances that whether the respondent's use was in bad faith "can be left undecided".

89 In contrast, the SDRP provision requiring a complainant to merely establish the respondent's registration *or* use of the domain name in bad faith, has obviated the need for any of the Panels in the SDRP cases to explicitly determine whether the respondent's bad faith related to its registration or its use. Instead, the SDRP Panels have tended to deal with the two together, whether in finding that at least one and/or the other has or have been met (where bad faith was established), or as the case may be, that neither one or the other has been met (where bad faith was not established).

90 Unlike the difference in the SDRP language from the UDRP language with respect to the first condition to be proved by a complainant (which does not appear to have differentiated the analytical approach of the SDRP Panels from that of the UDRP Panels much with respect to the first condition), the differing SDRP language with respect to the third condition, on the other hand, seems to have liberated the SDRP Panels from having to make a pointed distinction between whether the respondent's bad faith related to its registration or its use, in a way unavailable to the UDRP Panels.

---

144 *Supra* n 136, at para 6.3.4.

145 *Supra* n 137, at para 6.9.

146 *Supra* n 134, at para 6.14.

147 *Telstra Corporation Limited v Nuclear Marshmallows*, WIPO Case No. D2000-0003, at para 7.4.

148 *Fábricas Agrupadas de Muñecas de Onil S.A. (FAMOSA) v Gord Palameta*, WIPO Case No. D2000-1689.

149 *Green Tyre Company Plc. v Shannon Group*, WIPO Case No. D2005-0877.

VII. Open Source Initiatives

91 Open source is more than a contemporary catchword of the IT community. It seeks to revolutionize the entire software industry by moving it away from a proprietary paradigm to a commons paradigm, and also promote transparency and openness in the development, implementation and use of software. Numerous governments have abandoned proprietary software in favour of equivalent open source products, because governments do not want to be beholden to proprietary software developers, and also because governments want the additional security of accessibility of source code.[150]

92 In the same spirit of openness, the Singapore government has relaxed its requirements in asserting intellectual property rights in products and services developed by commercial providers for the government. In its new Singapore Government IP Policy,[151] which came into force in July 2004, the Singapore government now allows these providers contracting with the government to retain some intellectual property rights in works, products or services developed for the government. The basis of the policy is that this optimizes the value of Singapore's intellectual property by allowing it to be exploited commercially by those who can do so, such as the commercial proprietors. The Singapore government has also indicated its intention to license government intellectual property rights to third parties for commercial purposes. For instance, many companies have benefited from map data licensed by the Singapore Land Authority to release innovative map-related products.[152]

93 It is submitted that in the same spirit as the open source initiative, the Singapore government should be prepared to release key intellectual property rights into the public domain, or to make them open source. Examples of these would be cartographical and directory mapping data, urban planning data, key economic statistical data, caselaw and legislation. If they become open source, this will enable downstream developers to access government intellectual property rights, to build on them and to share the fruits of their development for the betterment of Singapore. Yet, because they are open source (as opposed to public domain), the Singapore government continues to retain intellectual property rights in them and, by virtue of the open source licensing, continue to retain a measure of control over derivative works created with them. Sharing such works with the public eliminates the economic loss arising from duplicated efforts in creating separate derivative works from the same data in the public domain,[153] and encourages differentiation, not by the exercise of proprietary rights over the derivative works created from the works in the public domain, but from differentiations in the quality of the services that can be offered from the use of these works.

94 It is understood that the Singapore government has studied the issue of open source seriously and there is a confidential government paper about the use of open source software in government agencies. Of course, another approach is possible, such as that taken by the Venezuelan government's open source law. Coming into effect on January 2006, the law will mandate all public agencies to undertake a two year transition to open source software.[154] The Singapore Ministry of Defence has taken highly public and visible steps to move away from proprietary software. It remains to be seen what the public stand of the Singapore government is as regards the use and the promotion of the use of open source software within the public sector.

---

150 *See, e.g.*, ZD-Net, "Massachusetts to adopt "open" desktop" (1 Sep 2005), at http://news.zdnet.com/2100-3513_22-5845451.html (accessed 28 December 2005); CNet News, "Governments push open-source software" (29 August 2001), at http://news.com.com/2100-1001-272299.html (accessed 28 December 2005).

151 Ministry of Law and IPOS, *Optimising Intellectual Property: IP Management Guidelines for the Public Sector in Singapore* (July 2004).

152 Singapore Land Authority, "What We Do: Land Information", at http://www.sla.gov.sg/what_we_do/land_information/land_data_hub.html (accessed 29 December 2005).

153 *See, e.g.*, NetAction, "Government Promotion of Open Source Software" (1999), at http://www.netaction.org/opensrc/oss-whole.html (accessed 28 December 2005).

154 O'Reilly, *Venezuela Open Source*, at http://radar.oreilly.com/archives/2005/12/venezuela_open_source.html (accessed 23 December 2005).

Conclusion

95 Clearly Singapore IT law is an area that has not been spared the attention and effort required to respond to the constantly evolving IT industry and its impact on the way business is done and the marketplace in general. Despite such attention and effort, there remains and possibly there will always remain, work to be done, given the inherently dynamic nature of technology and the potentially varied human response to it, at times predictable and at times, not. It is not realistic to imagine that Singapore IT law can be developed to perfection at any point in time and therefore it is perhaps more meaningful to accept and live with the ongoing need to consciously and constantly evaluate and review existing IT law, even as it is being applied, so as to build as conducive and as modern as possible a legal infrastructure that promotes use of state-of-the-art technology with certainty and confidence in a way that enhances all manner of business and social activities in Singapore.