INFORMATION MANAGEMENT

Towards Consumer Data Protection Legislation in Singapore

Information privacy is commonly protected in three ways. The first is a mandatory legislative framework which allows organisations to collect and hold data, subject to certain legal obligations, while protecting the rights of individuals to information privacy (data protection). The second is a co-regulatory scheme administered by the Government and industry. The third comprises industry-based, self-regulatory codes which are voluntary business initiatives, not laws. Singapore is proposing general base-line data protection legislation applicable only to the private sector which will operate alongside existing sector-specific statutes that govern certain public and commercial sectors. The long awaited Consumer Data Protection Bill is expected in 2012, after five years of an inter-ministry review. This is long overdue in view of global commerce and networks and the prevalence of data protection laws in many countries, among which are Singapore's major trading partners. This article will review the limited data protection that Singapore offers prior to the proposed legislation, trace the reasons in support of specific laws and suggest how the proposed framework could benefit from the experience of well-respected international and national initiatives in the area of information privacy.

TER Kah Leng
LLM (Bristol);
Barrister (Lincoln's Inn), Advocate and Solicitor (Singapore);
Associate Professor, NUS Business School, National University of Singapore.

I. Introduction

1 The personal information that is collected by marketing and human resource departments of commercial organisations and data collecting companies about their customers, employees and other parties is a valuable asset and an important business tool. Personal information[1] may be needed for a variety of purposes: for completing

1 Such as name, address, telephone number and e-mail address, identity card number, user IDs and passwords, image data, educational and employment background, billing and transaction information, sensitive information (financial information such as salary, credit card and banking information) and other
(*cont'd on the next page*)

a transaction or payment, providing service support, marketing products, detecting and preventing security threats, participating in contests and surveys or applying for a job. These practices pose very real legal compliance issues for organisations handling personal information, particularly in countries with data protection laws which govern the collection, use and disclosure,[2] security and transfer to third parties[3] and third countries of personal information. These practices also raise issues related to the ethical and correct exploitation of personal information. Trust and confidence in privacy and security in an online environment, as much as the credibility of the merchant and trustworthiness of the transaction, are matters of real concern to customers.

II. Protection of information privacy

2 With such critical issues in mind, it is surprising that Singapore, a financial centre and nation aspiring to be an e-commerce hub, has not been in the forefront of enacting specific data protection laws. Data protection may be viewed as part of the right to privacy, giving the individual the right to know, and to exercise control over, how personal information is collected, used and disclosed. Privacy, however, is not a constitutionally protected right in Singapore. Instead, limited protection is given to personal information under a bewildering variety of sector-specific statutes[4] (numbering over 160), through self or co-regulatory industry codes of practice,[5] contractual obligations or the common law.[6]

---

information collected through "cookies", "beacons", embedded web links and other electronic data collection tools.

2 What is collected, how it is collected and how the use is disclosed. Can it be used for purposes other than that specified?

3 Raises security and protection issues.

4 There are provisions governing the handling of personal information by government agencies and private sector entities in the Official Secrets Act (Cap 213, 1985 Rev Ed) (confidentiality of government databases); Statutory Bodies and Government Companies (Protection of Secrecy) Act (Cap 319, 2004 Rev Ed); Banking Act (Cap 19, 2008 Rev Ed) (banking secrecy); Telecommunications Act (Cap 323, 2000 Rev Ed); Central Provident Fund Act (Cap 36, 2001 Rev Ed); Statistics Act (Cap 317, 1999 Rev Ed) and Electronic Transactions (Certification Authorities) Regulations (GN No S 650/2010) (privacy of subscribers).

5 *Eg*, the Code of Consumer Banking Practice incorporating the secrecy provisions of the Banking Act (Cap 19, 2008 Rev Ed) and adopted by the Association of Banks; Singapore Code of Advertising Practice; the Code of Practice of the National Association of Travel Agents in Singapore; and the Industry Content Code aimed at developing a culture of responsibility in the internet industry and encouraging industry self-regulation by laying down industry best practices that will complement existing regulations and codes of practice governing internet content in Singapore (the Singapore Information Technology Federation took the lead in adopting the Code into its Trustmark Code of Practice); the Telecom Competition Code

(*cont'd on the next page*)

3 Sector-specific statutes are of limited scope and application with regard to data protection. They contain secrecy and disclosure provisions which typically penalise the unauthorised release of personal information. Industry-specific codes[7] may be directly relevant but lack legal force and sanction. A good example is the Model Data Protection Code for the Private Sector ("Model Code") developed by the National Internet Advisory Committee ("NIAC") Legal Subcommittee in December 2002. The Model Code,[8] based on internationally recognised standards, is a voluntary co-regulatory scheme co-ordinated by the National Trust Council ("NTC") representing industry and the Government (Ministry of Trade and Industry). The Model Code has been incorporated into the accreditation criteria for the "TrustSg",[9] a nation-wide e-merchant trustmark intended to create a more secure online business environment. This is an initiative by the NTC and supported by the Infocomm Development Authority of Singapore ("IDA").[10] Currently, the trustmark programme is compulsory for all government ministries and agencies. Businesses accredited with the "TrustSg" seal displayed on websites and physical storefronts signify that they are compliant to a code of conduct representing fair business, marketing and advertising practices drawn from the Model Code and that they respect customer privacy by adhering to privacy principles and proper management of customers' personal data. They include informing customers of the policies and procedures for managing personal data, the purposes of the data collection, their use and the need for consent before disclosing to third parties.

4 Feedback from businesses indicate that the "TrustSg" accreditation has enhanced credibility, increased customer confidence and boosted online sales and market share.

---

requires licencees to take reasonable measures to prevent the unauthorised use of consumers' information; and the E-Commerce Code for the Protection of Personal Information and Communications of Consumers of Internet Commerce.

6 Indirect protection under the laws of confidentiality, harassment, private nuisance, trespass and defamation. In *X Pte Ltd v CDE* [1992] 2 SLR(R) 575, the High Court held that under the common law, personal data such as telephone and other bills and receipts may be protected from disclosure under a duty of confidence. See Michael Hwang & Andrew Chan, "Singapore" in *International Privacy, Publicity and Personality Laws* (Michael Henry ed) (London: Butterworths, 2001) at p 356.

7 Infocomm Development Authority of Singapore Code of Practice; Singapore Code of Advertising Practice; Code of Practice of the National Association of Travel Agents of Singapore.

8 Government Policy, structured after the Model Data Protection Code for the Private Sector, has been incorporated in the government instruction manuals.

9 www.trustsg.sg. As at April 2006, about 300 private sector and 50 public sector organisations in Singapore have been accredited.

10 An industry-led organisation which seeks to develop Singapore into a dynamic global infocomm hub by nurturing a competitive telecoms market and a conducive business environment.

5 The NTC also seeks to facilitate cross-border recognition of trustmarks and to internationalise "TrustSg" through the Asia-Pacific Trustmark Alliance. Members of the Asia-Pacific Alliance include operators in Korea, Japan, Philippines, Singapore, Taiwan, Thailand, the US and Vietnam.

III. The Model Data Protection Code for the Private Sector

6 The Model Code was based on the Canadian Standards Association's Model Code for the Protection of Personal Information, which was derived from the Organisation for Economic Co-operation and Development's ("OECD") Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)[11] ("OECD Guidelines") and the EU Data Protection Directive[12] ("EU Directive"). The Model Code is expected to facilitate electronic commerce in Singapore and the future enactment of specific data protection laws. In fact, Singapore's proposed consumer data protection framework is derived from the Model Code as well as the data protection laws of certain key jurisdictions which will be highlighted below. As such, the data protection principles underlying the Model Code, its objectives and content will be relevant to the proposed legal framework. The objectives of the Model Code are to: (a) strike a balance between the legitimate information needs of businesses and an individual's interest in data protection; (b) harmonise data protection principles in the private sector and (c) establish minimum standards for the protection of personal data.

A. Data protection principles

7 The underlying principle of information privacy is that all personal data must be obtained, used and processed "fairly and lawfully". The original version of the Model Code contains 11 data protection principles which have been framed in broad, flexible terms to facilitate application across sectors. These principles form the basis

11 The Organisation for Economic Co-operation and Development's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("OECD Guidelines"). The OECD Guidelines govern the protection of privacy and transborder flow of personal data and cover collection, notification, use, security, disclosure, access and correction. OECD is primarily concerned with the economic development of its Member States which include the US, many European countries, New Zealand and Japan.

12 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* ("EU Directive"). Although the leading data protection framework, the Directive is expected to be replaced by a new framework that can effectively tackle the privacy developments of the 21st century.

of the proposed legislation. They deal with the access, collection, processing, use and transfer of personal data.

Principle 1 – Accountability

An organisation is responsible for personal data in its possession or custody and must appoint an individual who will be accountable for the organisation's compliance with the principles.

Principle 2 – Specifying purposes

An organisation must specify and document the purposes for which personal data is collected and reveal such information to the individual at or before the time the data is collected or if not, within a reasonable time thereafter.

Principle 3 – Consent

The knowledge and consent of the individual is required for the collection, use, or disclosure of personal data to a third party. This is subject to a long list of exemptions.

Principle 4 – Collection limitation

Subject to various exemptions, the collection of personal data is limited to the specified purposes. Data must be collected by "fair and lawful" means.

Principle 5 – Limiting use, disclosure and retention

Subject to various exemptions, personal data is not to be used or disclosed to a third party for purposes other than those for which it was collected, unless the individual consents to such use or disclosure. An organisation must implement guidelines and procedures to retain and destroy personal data and the individual must have access to the personal data which is to be used in making a decision concerning him. Personal data must not be kept longer than is necessary to fulfil the specified purposes and must be destroyed, erased or made anonymous if no longer required.

Principle 6 – Accuracy

Personal data must be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used. Updates are only to be obtained where necessary to fulfil the purposes for which the data is collected.

Principle 7 – Security safeguards

Personal data must be protected by appropriate security safeguards against accidental or unlawful loss, unauthorised access, disclosure, copying, use or modification. Security

measures must be commensurate with the risks and consequences of disclosure so that more sensitive data must be safeguarded by a higher level of protection. An organisation must exercise care in preventing unauthorised access to the data (*eg*, allowing access only on a need-to-know basis, stressing the importance of maintaining confidentiality) and when disposing of personal data.

Principle 8 – Openness

An organisation must make readily available its policies and procedures for handling personal data, the name and address of the data controller, the means of gaining access to personal data and what personal data is made available to other organisations (including subsidiaries).

Principle 9 – Individual access and correction

Subject to exceptions, an individual must, upon his request, be informed of the existence, use and disclosure of his personal data and must be given access to that data. Access may be refused, for example, where it would lead to disclosure of the personal data of another person; or when a government investigatory body or agency objects to the disclosure or for public policy, legal, security or commercial proprietary reasons. An individual is entitled to challenge the accuracy and completeness of his personal data and have it amended as appropriate.

Principle 10 – Challenging compliance

An individual is entitled to challenge compliance with the 11 principles of data protection and the organisation must investigate all complaints. Where the complaints are justified, the organisation must take appropriate measures, including amending its policies and procedures.

Principle 11 – Transborder data flows[13]

An organisation may transfer personal data to someone in a foreign country only if: (a) the organisation reasonably believes that the recipient is subject to a law, binding scheme or contract which upholds principles for fair handling of the data which are substantially similar to the principles in the Model Code; (b) the individual consents to the transfer; (c) the transfer is necessary for the performance of a contract between the individual and the organisation or for the implementation of

13 Adapted from Principle 9 of the Australian National Privacy Principles (Schedule 3, Privacy Act 1988). Principle 11 does not appear in the final version of the Model Data Protection Code for the Private Sector.

pre-contract measures taken at the request of the individual; (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; (e) all of the following apply: the transfer is for the benefit of the individual, it is impracticable to obtain his consent to the transfer, if it were practicable to do so, the individual would have consented or (f) the organisation has taken reasonable steps to ensure that the data it has transferred will not be held, used or disclosed by the recipient inconsistently with the principles of the Model Code.

B. Rights and obligations

8 The main obligations of the organisation under the Model Code include establishing and updating policies and procedures to protect personal data,[14] specifying the purposes for which the data is collected in documented form, obtaining the informed consent of the individual[15] (subject to permitted exemptions), collecting, using and disclosing such personal data as is necessary for the specified purposes (subject to permitted exemptions) and ensuring that the data is accurate, complete and up-to-date as is necessary for the specified purposes. The organisation must also ensure that its policies and procedures are implemented by third parties to which data collection is outsourced.

9 The rights of the individual include being informed of the purposes for which the data is collected at the point of collection and the organisation's policies and procedures for handling personal data, the right of access to personal data and the right to challenge its accuracy and completeness and to have any complaints investigated and the record amended. However, the organisation may refuse access to personal data in the circumstances stated in Principle 9 above.

C. "Personal data" and "data processing"

10 The Model Code regulates personal information in the form of electronic data and hence the term "personal data" is used. "Personal data" is defined as "data in an electronic form which relates to a living person who can be identified from those data or from those data and other information which are in the possession of, or likely to come into

14 Appropriate safeguards are needed to protect against accidental or unlawful loss, as well as unauthorised access, disclosure, copying, use or modification. The more sensitive the data, the greater the protection that is needed.

15 Consent need not be obtained directly from the individual unless it is sensitive data. It may also be implied, *eg*, the use of passwords, encryption, security clearance and limiting access to employees.

the possession, of the organisation". Since the Model Code covers "data in electronic form", it applies only to the processing of data wholly or partly by automated means and excludes data which is processed in a non-automated way, that is in a traditional paper based manual filing system. However, personal data kept in non-electronic form (manual data) which is subsequently converted to electronic form, will be subject to the Model Code thereafter. Organisations may, however, voluntarily submit their manually-recorded personal data to the operation of the Code.

11 The Model Code applies to a wide variety of "data processing activities".[16] It covers any personal data processed or controlled in Singapore, regardless of whether the organisation is within Singapore. It applies to all individuals (data subjects), whether or not they are resident in Singapore. Access and correction rights are not restricted to Singapore residents. Organisations cannot transfer any data which would involve a loss of control over the data, to any recipient whether within or outside Singapore unless certain conditions are met. Certain types of data and certain types of data processing may be exempted from some or all of the data protection rules. Certain "data processing activities" which are exempted include processing required by any law or court order, any processing that is necessary to safeguard national and public security, national defence, the national financial interest and processing of employment data. The NIAC Legal Subcommittee excluded employment data as it considered this to be burdensome to employers and likely to affect their competitiveness. However, the Subcommittee noted that the EU had criticised Australia for exempting employment data as such information was often very sensitive and should be protected. The Canadian Personal Information Protection and Electronic Data Act 2000 also excludes general employment information such as name, title, business address and telephone number from the definition of personal information.

D. Comments on the Model Code

12 Principle 11 of the Model Code above allows transborder data flows in certain situations, one of which is where the recipient upholds data protection principles which are substantially similar to the principles in the Model Code. In view of its exclusion from the final version, it is questionable whether compliance with the Model Code is adequate to meet the EU's requirement for transborder data flows. This will be discussed below.

16 Any operation performed upon personal data such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

13 A second observation is that there is a need to enforce a safer environment for data privacy which industry codes, lacking legal force, are unable to achieve. There must be a government regulatory authority to monitor and enforce data privacy. Under the Model Code, aggrieved individuals can complain directly to the organisation concerned, and if the complaint is not resolved, they may approach the NTC's Authorised Code Owners such as the Consumer Association of Singapore ("CASE") and CommerceNet which may assist in resolving the dispute through mediation, issuing a warning to the organisation in question or removing the organisation in breach from the "TrustSg" accreditation scheme. Alternatively, individuals may bring a private action against the organisation under the Consumer Protection (Fair Trading) Act[17] for engaging in an unfair trade practice by making a false claim regarding its privacy practices. But this does not directly protect data privacy or offer redress. The absence of an effective enforcement authority will be redressed in the proposed data protection laws.

IV. Rationale for specific data protection laws

14 As noted above, the framework prior to the Consumer Data Protection Bill is at best voluntary and lacks the force of law. It comprises numerous statutory provisions dealing with the confidentiality of personal information in the government and particular sectors together with the Model Code and other self-regulatory industry codes of practice for the private sector. It is a framework lacking in uniformity of approach. Furthermore, the statutory provisions deal with the more traditional forms of processing such as collection and disclosure without dealing with developmental issues such as accuracy, rights to access and correction, data security and new technology. It means that each technological development will require amendments to be made to the relevant statutory provisions. Such a fragmented approach, as the NIAC Legal Subcommittee pointed out, makes monitoring and auditing by the relevant authorities difficult and increases operational costs for global businesses. This is also confusing to consumers. [18]

15 Accordingly, the need for specific laws to regulate the collection, use, disclosure and transfer of personal data is long overdue. There are cogent reasons for saying so. There is a growing trend towards the enactment of comprehensive data protection laws around the world. Singapore is apparently the remaining developed nation without such laws. The policy has been to encourage sectoral regulation and industry self-regulation. At present, the e-commerce laws in Singapore provide

17 Cap 52A, 2009 Rev Ed.

18 National Internet Advisory Committee Legal Subcommittee, *Report on a Model Data Protection Code for the Private Sector* (2002) at paras5.15–5.17.

limited data privacy protection. Singapore has moved towards a knowledge and information based society and economy. Technology brings with it challenges to privacy and security that are involved in data protection, and requires specific laws not only to address these challenges but also to facilitate and promote e-commerce. A comprehensive legal framework will create certainty, and increase business reputation, competitiveness and customer confidence. Recently, consumer concerns about information privacy invasions have surfaced. Consumers feel uneasy about their personal information being collected or sent over computer networks. They are seeking assurance that their personal data will not be misused in relation to marketing efforts, resulting in unsolicited telephone calls or e-mails offering financial services or products and inviting participation in surveys or lucky draws.

16 Another reason for introducing specific legislation is that the majority of Singapore's top ten trading partners in 2010[19] have specific data protection laws, if not some data protection laws in place. At the top of the list is Malaysia which recently enacted a privacy-specific Personal Data Protection Act 2010.[20] Singapore's second major trading partner, the EU, is the world's leader on data protection legislation. Its Data Protection Directive[21] has influenced data protection legislation in countries such as Taiwan and Hong Kong. Of particular significance is the EU's prohibition on the transfer of personal data by Member States to third countries which do not have an "adequate level of protection". To similar effect is the Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (1981) which prohibits transborder data flows to those countries which are not signatories to the Convention where the flow is likely to contravene the Convention's data protection principles. The Madrid

19 Ministry of Trade and Industry, *Economic Survey of Singapore 2010* (February 2011).

20 Incorporating the data protection principles of consent, collection, usage, notice and choice, disclosure, security, retention, data integrity and access.

21 It aims to protect the individual's right to privacy with respect to the processing of data and to enable the free flow of data among the Member States. The EU Directive requires all Member States to enact comprehensive data protection laws administered by their own data protection authority. Although based on the EU Directive, there are important differences in the law from country to country. The key principle underpinning data protection is that everybody should be able to control how information about them is used or, at the very least, to be aware of how this information is used by others. "Data controllers" – people or organisations holding information about individuals – must comply with the data protection rules in handling personal data, and individuals – "data subjects" – have corresponding rights. The EU Directive expands on the 1981 Council of Europe Convention 108, which itself has its origins in Art 8 of the European Convention on Human Rights. The EU Directive has a primary economic approach which reflects its first pillar and internal market background. Despite similarities, there are fundamental differences of approach.

Resolution on International Privacy Standards (2009) also deals with international data transfers. This raises the significant issue of whether Singapore's future data protection laws will satisfy the EU requirement of an "adequate level of protection" for data transferred to Singapore and onwards. Singapore has to keep abreast with the data protection regimes of her major trading partners. Hong Kong[22] and Taiwan have also included in their respective data protection laws, prohibitions on the transfer of data to countries without adequate data protection, apparently to ensure the free flow of personal data from EU Member States. Singapore's third largest trading partner, the People's Republic of China, issued the draft Information Security Technology – Guide of Personal Information Protection on 30 January 2011. This will be the first comprehensive law on the handling and transfer of personal information. The US, Singapore's fourth major trading partner, takes a sectoral approach to privacy regulation,[23] but has responded to the EU adequacy requirement by implementing voluntary US Safe Harbor Rules for American companies trading with the EU.[24] The US has also entered into the US-Swiss Safe Harbor Framework. Information privacy has also prompted data protection laws in Singapore's other major trading partners such as Hong Kong,[25] Japan,[26] South Korea,[27] Taiwan[28] and Thailand.[29] Accordingly, Singapore should consolidate the self-regulatory industry codes and the hundreds of statutory provisions into one general, comprehensive data protection legislation.

22 Although yet to be implemented.

23 Involving some very detailed sector-specific laws, state laws and Federal Trade Commission laws/regulations. Individuals have power to enforce in some cases. Data privacy is not comprehensively regulated in the US as the right to free speech under the First Amendment of the US Constitution takes priority over the right to privacy unlike the EU which prioritises privacy over free speech.

24 Since the US is regarded as not providing protection equivalent to the EU rules, this has led the US to negotiate "safe harbor" guidelines with the EU. When a US company signs up to this scheme, it agrees to follow seven principles of information handling and to be regulated by the Federal Trade Commission or other bodies.

25 The Personal Data (Privacy) Ordinance 1995 covers both public and private sectors and the processing of both automated and manual data.

26 The Act on the Protection of Personal Information 2003 protects personal data held by businesses. It was drawn from the OECD Guidelines and was supplemented by a recent Act on the Protection of Personal Data held by Administrative Agencies and the Act on the Protection of Personal Data held by Independent Administrative Legal Entities.

27 The Act on Promotion of Information and Communication Network Utilization and Information Protection of 2001 protects personal information held by certain industries. The first comprehensive data protection law, the Personal Information Protection Act was enacted on 29 March 2011.

28 Law Governing Protection of Personal Data Processed by Computers 1995 was amended by the Data Protection Act passed in April 2010 and likely to come into force sometime in 2011.

29 Thailand has a draft Privacy Act (yet to be finalised) whose approach is closely aligned with the EU Directive.

17 However, far from consolidating these into one uniform, comprehensive scheme, the proposal is to allow sector-specific statutes to operate alongside the proposed legislation. This is likely to create uncertainty and cause consumer confusion. Notwithstanding this, having some specific data protection laws will ensure compatibility with international standards developed by the EU, the Council of Europe and the OECD, which have greatly influenced the national legislation enacted by Singapore's major trading partners. Singapore being an international financial and commercial centre and host to multinational companies should have laws consistent with European and international data protection standards that facilitate commerce while protecting personal data. This will ensure that data flows and trade will not be impeded by the requirements of national and supranational data protection laws. It will instead demonstrate that data protection is a shared value Singapore has in common with other developed and developing nations. In fact, the Ministry of Information, Communications and the Arts ("MICA") recognised in its Public Consultation Paper: *Proposed Consumer Data Protection Regime for Singapore*[30] ("MICA's Public Consultation Paper") that the proposed data protection regime will bring economic benefits and put Singapore on par with advanced economies with data protection laws. "This will strengthen and entrench Singapore's position as a trusted hub for businesses, a key national economic strategy for Singapore."[31] In fact, at a media briefing, MICA said that internet companies such as Google or Yahoo! might have been deterred from hosting their data here by the absence of a general data protection law.[32]

V. Towards a legal framework for data protection

18 The NIAC Legal Subcommittee recommended a uniform, comprehensive data protection regime as "part of a package of rules to facilitate trade and the growth of E-Commerce generally".[33] The Subcommittee was inspired by the unanimous conclusions of the UK, Canadian and Australian Law Reform inquiries that self-regulation provides inadequate protection for information privacy.[34] However, as data protection is "a complex issue, having a potentially extensive impact on many stakeholders", an Inter-Ministry Data Protection Subcommittee was set up to find a suitable regulatory regime that could

30 13 September 2011.

31 Public Consultation Paper issued by the Ministry of Information, Communications and the Arts: *Proposed Consumer Data Protection Regime for Singapore* at para 1.3.

32 *The Straits Times*, 14 September 2011.

33 National Internet Advisory Committee Legal Subcommittee, *Report on a Model Data Protection Code for the Private Sector* (2002) at paras 5.19 and 5.20.

34 National Internet Advisory Committee Legal Subcommittee, *Report on a Model Data Protection Code for the Private Sector* (2002) at para 6.7.

best address Singapore's privacy concerns, commercial requirements and national interest.[35] After years of deliberation, the review concluded in favour of Singapore's overall interests in having a data protection regime to protect personal data against unauthorised use and disclosure for profit. On 14 February 2011, the Minister for Information, Communications and the Arts announced plans to introduce a new Data Protection Bill in early 2012. This will provide a "baseline standard for data protection in Singapore" and seek to curb "excessive and unnecessary collection" by businesses of individuals' personal data, require an individual's consent to disclose personal data, safeguard sensitive data and possibly impose criminal sanctions for breaches. A Data Protection Council will be set up to oversee the implementation of the legislation. The Minister hoped that the proposed law will also encourage businesses such as cloud computing firms, which upload information and share resources online, to locate their business here. However, the data-mining industry called for a lighter touch, arguing that the data that was mined and sold such as company, residential and government information, was harvested from public websites or name cards. This was quite unlike stealing information and then reselling it.[36] On the other hand, there have been growing concerns over certain breaches of confidentiality relating to personal data involving the leakage of personal contacts of graduates from a tertiary institution and the sale of personal contact information of key government officials.

19 The Government's concern is echoed in MICA's Public Consultation Paper that a sectoral approach may not be able to address adequately the increasing public concern over data protection across multiple sectors and that general data protection legislation is needed.[37] The lack of a data protection regime could hinder cross-border flow of data and Singapore's development as a global hub since data protection is a basic feature in most economies and sophisticated clients do expect their personal data to be protected.[38] Hence, the key objectives in the proposed law are: (a) to ensure adequate safeguards for personal data and to enhance consumer trust in the private sector; and (b) to strengthen Singapore's overall economic competitiveness and enhance her status as a trusted hub and choice location for global data management and processing services.[39] This is a pragmatic approach

35 *Singapore Parliamentary Debates, Official Report* (15 February 2007) vol 82; *Singapore Parliamentary Debates, Official Report* (19 January, 2009) vol 85.

36 *The Straits Times* (18 February 2011).

37 Ministry of Information, Communications and the Arts, Public Consultation Paper: *Proposed Consumer Data Protection Regime for Singapore* at para 2.8.

38 Ministry of Information, Communications and the Arts, Public Consultation Paper: *Proposed Consumer Data Protection Regime for Singapore* at paras 2.09 and 2.10.

39 Ministry of Information, Communications and the Arts, Public Consultation Paper: *Proposed Consumer Data Protection Regime for Singapore* at para 3.1.

motivated by economic reasons and consumer protection that is necessary to promote Singapore as a trusted global hub for data services.

A. Drawing on international standards

20 The experiences of other economies with comprehensive data protection laws suggest that the model for Singapore should share the following characteristics: (a) be comprehensive, principles based, generally compatible with international principles and open to global trends in order to plug into the global economy; (b) have minimal exemptions; (c) overseen by a regulatory authority with enforcement powers; and (d) provide co-operation among privacy enforcement bodies where the breach involves more than one economy. In fact, the Asia-Pacific Economic Cooperation ("APEC") Forum[40] suggested that member economies "should consider developing cooperative arrangements and procedures to facilitate cross-border cooperation in the enforcement of privacy laws".[41] Very few privacy laws have provisions facilitating global co-operation and enforcement. Singapore could become a model for Asia, if not for the world.

21 The proposed law should align itself with highly respected international standards and frameworks derived from the OECD Guidelines (1980), the Council of Europe Convention (1981), the EU Directive (1995), the APEC Privacy Framework (2005) and the Madrid Resolution on International Privacy Standards (2009).[42]

22 The OECD Guidelines, along with the Council of Europe Convention and EU Directive, have influenced national legislation on privacy and personal data protection in many countries. The EU principles are regarded as a model for good data protection practices.[43]

23 Although the EU Directive has influenced the APEC Privacy Framework, the latter is viewed as incorporating weaker international

40 Asia-Pacific Economic Cooperation ("APEC") is a forum for facilitating economic growth, trade, co-operation and investment in the Asia-Pacific region.

41 "APEC Privacy Framework: Facilitating Business and Protecting Consumers Across the Asia-Pacific" in APEC e-Newsletter vol 7, January 2006.

42 Adopted by the Data Protection Authorities of 50 countries gathered within the 31st International Conference of Data Protection and Privacy on 6 November 2009. A group of ten large multinational companies (Oracle, Walt Disney, Accenture, Microsoft, Google, Intel, Proctor & Gamble, General Electric, IBM and Hewlett-Packard) have signed a declaration of support for the adopted joint proposal on international standards on privacy and data protection. Also supported by the group on data protection from the Council of Europe.

43 EU Data Privacy Principles: fairly and lawfully processed; processed for limited purposes; adequate, relevant and not excessive; accurate and up-to-date; not kept for longer than is necessary; processed in line with your rights; secure; not transferred to other countries without adequate protection.

standards and is the least robust. The Framework merely provides voluntary guidance to member economies[44] for "the development of appropriate information privacy protections ensuring the free flow of information in the Asia-Pacific region". The nine APEC privacy principles are generally consistent with the OECD Guidelines. Part B of the Framework contains cross-border privacy rules. Principle 9 on Accountability covers the transborder flow of information. Member economies have either adopted data protection laws since the late 1980s or are increasingly adopting these laws. The Model Code, although issued earlier, is generally consistent with the APEC Framework. Although the Model Code does not recognise the right to privacy under APEC's Principle 1 on Preventing Harm, it seeks to prevent the harm resulting from breach of data privacy.

24 The Madrid Resolution, the most recent initiative, brings together all the multiple approaches possible in the protection of privacy, integrating legislation from all five continents. The proposal includes a series of principles, rights (access, rectification, cancellation and objection) and obligations (security of personal data, confidentiality) that any privacy protection legal system must strive to achieve. The purpose is to effectively protect privacy at an international level as well as to ease the international flow of personal data, essential in a globalised world. Among the basic principles are those of loyalty, legality, proportionality, quality, transparency and responsibility, common to the various privacy laws and enjoying wide consensus in their corresponding geographical, economic or legal application environments. It is significant that the document articulates pro-active measures by states to promote better compliance with data protection laws and for supervisory authorities to provide, *inter alia*, procedures aimed at preventing and detecting fraud or offer awareness, education and training programmes and for different states to co-operate and co-ordinate their activities. The document defines sensitive data as "data that affects the most intimate side of a person or whose misuse can originate an illegal or arbitrary discrimination or may imply a severe risk for the person". Certain requirements are to be met for the legal collection, preservation, use, revelation or erasure of personal data (*eg*, prior free, unequivocal and informed consent for the data subject). Last but not least, international data transfers may be performed when the receiving state offers at least the level of protection foreseen in the document or when the transferor can guarantee that the recipient will offer the required level of protection (*eg*, through appropriate contractual clauses).

---

44 Twenty-one members being Australia, Brunei Darussalam, Canada, Chile, People's Republic of China, Hong Kong, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, the Philippines, Russia, Singapore, Taiwan, Thailand, the US and Vietnam.

25 In drafting the new data protection legislation, Singapore has drawn on the Model Code and referred to the APEC Privacy Framework together with the data protection laws of the EU, the UK, Hong Kong, Canada and New Zealand.[45] However, these jurisdictions have advanced to the next stage of reviewing their data protection laws to bring them up to date with new technology and business practices. It is timely for Singapore to capitalise on these developments.

B. Policy

26 The policy considerations underpinning the proposed data protection regime are five-fold: (a) striking a balance between consumer protection and the commercial use of personal data for legitimate purposes; (b) advancing Singapore's economic interests by strengthening her competitive advantages as a trusted data hosting hub; (c) keeping compliance costs manageable, particularly for small and medium sized enterprises ("SMEs"); (d) ensuring consistency with international standards and (e) facilitating cross-sector data flows by applying minimum standards of data protection across all sectors.

27 Data protection could take the form of either "heavy" prescriptive legislation or "light-touch" legislation. Singapore will adopt the latter and enact baseline law applicable to all organisations except those in the public sector. This will operate concurrently with existing sectoral regulations to ensure a minimum standard of data protection while providing flexibility for specific sectoral needs. This is viewed as a more balanced approach than enacting data protection laws which either supersede or are superseded by sectoral regulations.[46]

28 For the purpose of overseeing compliance with the new laws and to promote education and awareness on proper data protection processes, a Data Protection Commission ("DPC") will be established.

C. Comment

29 Unlike the personal data privacy regimes elsewhere, Singapore's proposed general legal framework is not comprehensive in terms of scope of application. It will operate alongside existing sectoral legislation and apply only to the private sector. This is similar to the Malaysian Personal Data Protection Act 2010 which exempts from its application the Federal and State Governments and confines its

45 Ministry of Information, Communications and the Arts, Public Consultation Paper: *Proposed Consumer Data Protection Regime for Singapore* at para 3.6.

46 Ministry of Information, Communications and the Arts, Public Consultation Paper: *Proposed Consumer Data Protection Regime for Singapore* at para 3.8.

application to the regulation of the processing of personal data in the context of commercial transactions by data users. Telcos have argued that there should not be dual regulations for any organisation which is already regulated by sector specific regulation. Only the latter should apply. It is also feared that the new regime would impose unnecessary burden and costs as the sector is already subject to infocomms regulations.[47]

30 However, there are cogent reasons for suggesting a consistent national framework for both public and private sectors, as is the position under the EU Directive, the Australian Federal Privacy Act 1988 (Cth) and the Hong Kong Ordinance, to name a few. MICA supports its proposal to exempt the public sector with the reason that public sector rules are "consistent with the principles of the Model Code" and "accord similar levels of protection for personal data as the proposed data protection law".[48] As it stands, sectoral protection of personal data is of limited scope and application and the great diversity of laws creates confusion. It may better serve the interests of certainty and uniformity for data protection principles and sectoral legislation to be merged into a single legislative framework. Within this framework, the recognition of industry codes of practice may result in "regulating less but better". This is seen in Hong Kong where sectoral codes acquire legal basis once they are formally approved. Sectoral codes may effectively complement a general regime by providing more detailed protection for certain files such as telecommunications, police files or consumer credit records. Voluntary code-based privacy protection that embraces OECD Guidelines can demonstrate the flexibility that is conducive to global commerce. This is also apparent under the Malaysian Personal Data Protection Act 2010 where the Ministry of Information, Culture and Communications will issue detailed guidelines and codes of practice which will have the force of law. These will be critical in clarifying more precisely the scope of application and will set out practical recommendations for compliance. A key role in formulating such codes is expected to be played by the private sector, through data user forums prescribed in the Act. Singapore's proposed law could similarly provide for the DPC to assist in drawing up sectoral codes of conduct by trade and professional associations.[49]

D. Scope of application

31 The proposed Act provides a minimal baseline standard for the collection, use and disclosure of personal data by all persons, companies

47 *The Business Times* (1 November 2011).

48 Ministry of Information, Communications and the Arts, Public Consultation Paper: *Proposed Consumer Data Protection Regime for Singapore* at para 3.18.

49 As under Art 27 of the EU Directive.

and organisations[50] in the private sector in Singapore (collectively referred to as "organisations"). The proposed law does not make a distinction between data controllers[51] and data processors[52] (unlike some jurisdictions like the EU) but applies to organisations which have personal data either in their "custody or control". It will hold any organisation responsible for personal data under its custody or control, including personal data that is not in the organisation's custody but under its control. Hence, an organisation outsourcing the collection and/or processing of personal data is still responsible for the management of such data. So is the company that is processing personal data on an outsourced basis as it is deemed to have control over the personal data.

32 Data regarding individuals residing in a particular jurisdiction may be accessed online and collected from anywhere. The UK Data Protection Act[53] extends to data processing activities carried out by overseas organisations through UK-based servers or cookies installed on UK users' computers. The European Commission has expressed the view that with technological advancement, privacy standards for Europeans should apply independently of the location in which their data is being processed.[54] MICA is therefore considering whether or not to regulate personal data that is collected in Singapore by organisations located overseas, bearing in mind the practical problems of carrying out investigations and enforcement proceedings against the collecting organisation which has no presence in Singapore. In other words, should the proposed law cover only organisations in Singapore or should it also cover data collection and processing in Singapore regardless of the location of the organisation?

E. Individuals – Data subjects

33 The NIAC Legal Subcommittee subscribed to the OECD's view that individual integrity and privacy are to be differentiated from the integrity of a group of persons or corporate security and confidentiality. Hence, the Model Code applies only to natural, living individuals and not to legal entities such as corporations or associations. The same

50 Defined to include a natural person, a trust and any company or association or body of persons, corporate or unincorporated, but does not include a natural person acting in a personal (matters relating to the individual concerned) or domestic (matters referring to the home or family of the individual concerned) capacity.

51 Organisations that are in control of personal data and decide on the purposes for which it will be used and the manner in which it will be used.

52 Organisations that hold data on behalf of the data controller and can only use data in accordance with instructions given by the data controller.

53 1998, c 29.

54 In a speech delivered on 16 March 2011 by the Vice-President of the European Commission.

approach will be adopted in the proposed legislation and the new law will refer to data subjects as individuals.

34 The new Act should protect all individuals irrespective of their citizenship, residence or presence in the country. Access and correction rights should be available regardless of the individual's place of residence.

F. Data protection principles

35 The proposed legislation should be principles based, consistent with international standards and trends, create flexibility and enable the various sectors to achieve their objectives efficiently. Content principles should comprise core privacy principles and enforcement objectives. The privacy principles will ensure that personal data is processed in a way that protects the interests of individuals. All organisations are required to comply with the principles unless the processing falls within one of the listed exemptions. The enforcement objectives should ensure compliance, help individuals in the exercise of their rights and provide appropriate redress to them when rules are infringed.

36 The adoption of the 11 principles of the Model Code should form a sound basis for the proposed law.

37 In line with international best practices, MICA has proposed that the new regime be based on consent, purpose and reasonableness.

G. General rules and exclusions

(1) General exclusions

38 The proposed law should consider the range of exemptions for certain data processing activities and consider taking a "risk-based" approach to data protection which emphasises protecting data that is of greatest risk of abuse as opposed to an approach which restricts use of data whether associated with risk or not. The NIAC Legal Subcommittee surveyed the data protection regimes in various countries and incorporated an exhaustive list of exemptions of certain types of data and data processing from some or all of the provisions in the Model Code. The proposed legislation appears to be adopting the same approach, rather than follow the Hong Kong Ordinance which is comprehensive, with very few exemptions compared with other national data protection legislation.

39 MICA has proposed general exclusions from the application of the proposed law, taking into account international practice and Singapore's context. They are:

(a) personal data recorded in a court document;

(b) personal data that is contained in a record that has been in existence for at least 100 years or under the control of a public agency or its agent;

(c) where personal data has been made available by a public agency to a specific organisation or to the public generally;

(d) where data is collected, used or disclosed by a news organisation in the course of a news activity;

(e) where data about an individual's business contact information is collected, used or disclosed solely for the purpose of enabling the individual to be contacted in relation to his employment, business or profession.

40 MICA is also seeking feedback on whether there should be exclusions for artistic or literary purposes in light of Canada's exclusion for biographies, plays, musical compositions, photography, *etc*. MICA, however, finds considerable practical difficulty defining such exclusions to meet legitimate needs. In this regard, the Minister will have powers to make general exemptions and to amend the list of exclusions.

(2) General rules

41 Turning to the general obligations of organisations, they fall into four broad areas:

(a) transparency of processes;

(b) collection, use and disposal of personal data;

(c) accuracy, protection and retention of personal data; and

(d) access to and correction of personal data.

(a) Transparency of processes

42 Organisations must be transparent and open to customers in their policies and practices relating to the management of personal data. They must designate one or more employees with the task of ensuring compliance and disclosing to consumers their business contact information.

(b) Collection, use and disposal of personal data

43 The management of personal data involves the life-cycle of collection, use/processing, disclosure, retention and deletion of personal data.

CONSENT

44 An organisation may only collect, use or disclose personal data with the individual's consent[55] and for a reasonable purpose[56] which the organisation has disclosed (either verbally or in writing) to the individual on or before collecting his personal data or unless this is permitted under the Act or any other written law. The organisation must disclose the business contact information of an officer or employee who is able to answer queries about the collection of the data.

45 Where an organisation collects data from another organisation without the consent of the individual, the collecting organisation must provide the other organisation with sufficient information regarding the purpose of the collection on or before the collection to enable the other organisation to determine whether the disclosure is in accordance with the Act.

46 Consent should not be obtained for a purpose beyond what is needed to provide the product or service. Consent may be express or implied. It may be implied as where a patient gives his personal particulars when making a medical appointment. He will be deemed to have consented to the collection and use of his personal data by the medical organisation for the purpose of seeking medical treatment. Consent may also be deemed in the context of enrolment for or coverage under an insurance, pension, annuity, provident fund, benefit or similar plan, policy or contract, under which the individual is a beneficiary or has an interest as an insured under the plan and is not the applicant for the plan, policy or contract. MICA takes the view that requiring explicit consent could be onerous and detract from the objectives of including the individual under the plan, policy or contract.

47 MICA is seeking views on whether to adopt the "opt-out" approach of British Columbia in relation to the issue of consent. This means that when an individual is notified of an organisation's intent to collect, use and disclose his personal data and if he does not register any objections within a reasonable time, he is deemed to have consented by not "opting-out". While such an approach may be more cost-effective for organisations, MICA noted that this would place an unreasonable burden of establishing consent on the individuals.

55 In limited circumstances, prior consent need not be obtained as in the case of medical emergencies where the individual is unable to give consent.

56 A purpose which a reasonable man would consider appropriate in the circumstances, *eg*, it would be unreasonable for a readership survey to ask for the annual income of the respondent.

48 Consent may be withdrawn at any time unless such withdrawal would frustrate the performance of a legal obligation or where consent has been given to a credit bureau for the purposes of creating a credit report.

49 An individual's consent will be vitiated where the organisation provides false or misleading information with respect to the collection, use or disclosure or if it employs deceptive or misleading practices. Any consent given as a condition of supplying goods or services beyond what is necessary to provide the goods or services will be void.

EXCEPTIONS TO THE REQUIREMENT OF CONSENT

50 In addition to the proposed general exclusions set out above, specific exclusions from the requirement of consent are set out below:

(a) an investigation by a public agency or law enforcement agency in Singapore;

(b) research activities (including business analytics and statistical research);

(c) mergers and acquisitions involving organisations;

(d) where the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way, *eg*, in the case of medical emergencies where the individual is unable to give consent; where the collection is necessary to respond to an emergency that threatens the life, health or security of an individual; or where it is reasonable to expect that the collection with the consent of the individual would compromise the availability or accuracy of the personal data and the collection is reasonable for an investigation or legal proceeding;

(e) under the Infectious Diseases Act,[57] healthcare professionals are required to collect and disclose information from a patient to the Director of Medical Services for the purpose of preventing the spread of an infectious disease;

(f) where the collection is required or authorised by law, or where the data was disclosed to the organisation without consent for purposes which the Act does not require consent;

(g) when the personal data is available to the public, or when it is collected by observation at a performance, a sports meet or similar public event at which the individual voluntarily appears. This recognises that it would be impractical or

57 Cap 137, 2003 Rev Ed.

unproductive to prohibit such sharing of data. However, in view of a multitude of data sources (*eg*, telephone directories and newspapers) that could be considered publicly available, the DPC will provide guidance on the types of sources that would be considered as such;

(h) employee personal data[58] for the purposes of establishing, managing or terminating an employment relationship between the organisation and the individual and where the collection is reasonable for the specified purposes. The organisation must notify the individual of the collection and the purposes for the collection;[59]

(i) the collection of members' personal data for identification purposes or for internal circulation, *eg*, photographs for identification passes or for newsletters;[60]

(j) to enable the relevant organisations to perform their functions effectively, *eg*, a credit bureau compiling the credit report need not obtain additional consent when an individual has consented to disclosure of his personal data for a credit report; an organisation collecting or paying a debt or providing legal services to a third party where consent might impede the effective execution of these activities; organisations under the purview of the National Council for Social Services providing financial assistance or social services to individuals or their families need not obtain consent to collecting data for the purpose of determining eligibility for such assistance or service;

(k) where an individual acting in a personal or domestic capacity provides personal data relating to another party to an organisation for the provision of services to the individual or for the purpose of determining the individual's suitability to receive an honour, award or similar benefit or to be selected for an athletic or artistic purpose;

(l) where an organisation outsources the collection or processing of personal data, it will not be necessary to obtain the consent to transfer the personal data to the second organisation as long as the individual previously gave his consent to the first organisation and the sharing is solely for the purposes for which the information was collected and to assist the first organisation outsourcing the work.

58 Does not include personal data that is not about an individual's employment.

59 Such differential treatment of employee data is also apparent in the Personal Information Protection Act of British Columbia.

60 Ministry of Information, Communications and the Arts takes the view that the burden of obtaining consent outweighs the merit of protecting such data, particularly if it is intended for internal circulation. It is seeking views on this.

USE/PROCESSING

51 The use or processing of the data must be reasonable and only for the purposes for which the consent was obtained. The reasonableness of the purpose will be determined objectively by what a reasonable person would consider appropriate in the circumstances. Unless it is not required under the Act, fresh consent must be obtained if the data is to be used for a purpose other than that for which consent was given.

52 The Act prescribes exceptions to the use of data without prior consent. These are similar to those relating to the collection of personal data without consent, as discussed above.

53 It is interesting that the Hong Kong Personal Data (Privacy) (Amendment) Bill 2011 provides for an "opt-out" facility by organisations that maintain databases or mailing lists for direct marketing purposes or use a third party to do so. There is a requirement for data subjects to be informed of their right to "opt-out" on first use of their data for marketing purposes and a right to "opt-out" at any time subsequently.

54 The Hong Kong Personal Data (Privacy) (Amendment) Bill 2011 also created a qualified exemption allowing the use of personal data for the purpose of a due diligence exercise conducted in connection with certain proposed business transactions that involve the data user. On completion of the exercise, it must be returned to the transferor (data user) and any record of it must be destroyed. The exemption applies if it is not practicable to obtain the consent of the individual for the transfer.

DISCLOSURE

55 Disclosure must also be in line with the purpose for which the consent was obtained, unless otherwise permitted under the Act or required under any other written law. The exceptions are similar to those applicable to collection and use discussed above. Other unique situations where consent is not needed for disclosure are:

(a) when the data is required by a public agency or law enforcement agency in Singapore for the purpose of an investigation into an offence or other infringements of the laws of Singapore or when the information to be disclosed relates to national security, defence, public security, the conduct of international affairs or similar matters of national interest;

(b) when the purpose of the disclosure is to comply with a subpoena, warrant or order issued or made by a court or the

disclosure is made to an advocate and solicitor who is representing the organisation; disclosures to police officers or any other officers of the Ministry of Home Affairs authorised to collect personal data for the purpose of their functions and duties under any written law; where there are reasonable grounds for believing that compelling circumstances exist that affect the health or safety of any individual[61] or when the disclosure is for the purpose of contacting the next-of-kin or a friend of an individual who is injured, ill or deceased;

(c) disclosure to prescribed archival institutions, *eg*, National Archives, if the collection is reasonable for research or archival purposes;

(d) disclosure to other organisations for research purposes, including statistical research and business analytics, when it is impracticable to seek consent and the research purpose cannot reasonably be accomplished unless the personal data is provided in an individually identifiable form. However, the personal data must not be linked to other information that could be harmful to the individuals identified by the personal data and the benefits to be derived from the linkage are clearly in the public interest. Conditions relating to policies, procedures, security and confidentiality of the data have to be adhered to. Furthermore, the personal data cannot be used to contact individuals to seek their participation in the research. Organisations using the personal data for research must remove or destroy individual identifiers at the earliest reasonable opportunity. MICA stressed that this exception applies purely to research activities which will support the drive to make Singapore a hub for such emerging industries. It does not permit organisations to collect, use or disclose personal data for marketing purposes; and

(e) the sharing and transfer of personal data about customers, employees, shareholders, directors and shareholders that is required in an agreement relating to a merger or an acquisition. Such information is required to evaluate and complete the business transaction. The individuals must be informed that the business transaction has taken place and their personal data has been disclosed to the other party. If the merger or acquisition is not completed, the prospective buyer must destroy or return the personal data it has collected to the organisation.

56 As for data sharing arrangements between businesses such as joint venture parties, corporate groups or franchising parties, these must

61 But the individual must be notified of the disclosure.

comply with the new laws but it is good practice to have a data sharing agreement in place. It should deal with the purpose of sharing data, data quality, security, retention, access requests and sanctions for breach. It is interesting to note that the UK Information Commissioner's Office published a new Data Sharing Code of Practice on 11 May 2011. The Code is designed to facilitate data sharing and although not legally binding, it sets out guidelines on when data can be shared and how it should be protected.

TRANSFER OF DATA – INTERNATIONAL TRANSFERS

57 In order to maintain trust and confidence of consumers in Singapore, they need to be assured of a similar level of protection when their personal data is transferred out of Singapore. This is significant with the increasing frequency of cross-border data transfers with market developments such as cloud computing[62] where data is held somewhere else, usually in a cheaper jurisdiction. In this case, the responsibility will be placed on the transferor organisation which has control over the data to ensure that appropriate measures are taken to protect the personal data. This is the "principle based" approach that Singapore prefers to take, as opposed to a prescriptive approach of requiring adequacy rulings for foreign regimes, such as that required by the EU.[63] However, if Singapore aspires to attract cloud computing business, it must ensure an adequate level of protection (consistent with the EU Directive) for European data transferring out of the European Economic Area to Singapore.[64] This will be further discussed below.

(c) Accuracy, protection and retention of personal data

58 The new legislative regime caters for three aspects of safeguarding personal data by providing rules on accuracy, protection and retention of personal data:

> (a) organisations are to make reasonable efforts to ensure that personal data that is collected is reasonably accurate and complete, if the data is likely to be used in decision making that will affect the individual or is likely to be disclosed to another organisation;

62 Defined by Hewlett Packard as "a delivery model for technology-enabled services that provides on demand access via a network to an elastic pool of shared computing assets (eg services, applications, servers, storage and networks) that can be rapidly provisioned and released with minimal service provider interaction. The entire vale can be bi-directionally scaled as needed to enable pay-per-use".

63 Companies could comply by using the updated 2010 EU-approved "model clauses" to protect personal data transferring out of the European Economic Area.

64 The Monetary Authority of Singapore has issued Circular No SRD TR01/2011 on Information Technology Outsourcing which addresses outsourcing activities, including cloud computing services, by financial institutions.

(b) to prevent data breaches and inadvertent disclosure by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, modification, disposal or other similar risks. Guidelines may be issued on suitable methods of protection that can be considered by organisations; and

(c) where personal data has been used in decision making affecting the individual, the organisation using that data has to retain that information for a sufficient period of time after using it to give the individual a reasonable opportunity to access the information. As soon as it is reasonable to assume that the purposes for which that data was collected are no longer being served by retention, the organisation must destroy that data or anonymise it. This is intended to strike the right balance between the need for retention and the requirement for deletion or anonymisation when the data is no longer needed for the specific purposes.

59 MICA is seeking views on whether organisations should be required to specify the retention period at the point of collecting the personal data.

DATA SECURITY

60 Under the new law, organisations are to protect personal data in their custody or under their control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or other similar risks.

61 In accordance with the principle that personal data should not be kept longer than is necessary for their intended purpose, the proposed Act should ensure that personal information should be disposed of in a secure manner, for example by using a professional data destruction company. Proper security measures should also be implemented to protect data against hacking and alteration, loss or destruction.

62 The importance of data security is highlighted by the recent high profile attacks on Sony, Sega and Nintendo. In the Sony incident during April 2011, the personal details of 100 million users of various gaming and online entertainment servers were compromised. Sony was forced to shut down its PlayStation network and Sony Online Entertainment service for a number of weeks. Such a security breach exposes Sony to civil claims and monetary penalties as well as class actions.

(d) Access to and correction of personal data

63 Individuals have the right to request access to their personal data held by an organisation. It must assist the individual in obtaining access, provide information about how the data has been and is being used and provide the names of the individuals and organisations to whom the personal data has been disclosed. Credit bureaus should also provide the individual with the names of the sources from which they received the personal data, unless it is reasonable to assume the individual can ascertain those sources. Individuals can also ask organisations to correct any inaccurate data which is under their control. Such corrected data must be sent to any other organisation to which the personal data was disclosed during the year before the date the correction was made. The other organisation is required to correct the data under its control. A reasonable fee may be charged for costs incurred in allowing access to and correcting the data.

64 Under the new law, an organisation is not allowed to provide the individual with access to his personal data in the following circumstances:

(a) where the data is subject to legal privilege or if collected or created by a mediator or arbitrator in the conduct of a mediation or arbitration or if disclosure would reveal confidential commercial information which could reasonably harm the competitive position of the organisation;

(b) when the data was collected or disclosed without consent as permitted under the Act for the purposes of an investigation, national security, defence, public security, the conduct of international affairs or similar matters of national interest. Disclosure to the individual in these cases could compromise the investigations and operations of the relevant authorities;

(c) if the disclosure could reasonably be expected to threaten the safety or physical or mental health of another individual or cause immediate or grave harm to the safety, physical or mental health of the individual who made the request;

(d) when the disclosure would reveal personal data about another individual or the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to disclosure of his identity, the organisation would also not be allowed to provide access to the data; and

(e) in the case of frivolous or vexatious requests or where responding to the request would unreasonably interfere with

the operations of the organisation due to the repetitious nature of the requests or if the individual had previously waived the right to view a reference given for the purposes of an individual's education or employment.

H. Definition of "personal data" and "data filing" systems

65 Personal data may include any of the following: (a) information about an individual which can be used to identify a specific individual such as name, age, weight, height, religion, marital status, race, ethnic origin and colour, NRIC/FIN[65] or passport number, photographs, blood type, DNA code, fingerprints, education, salary or home address and telephone number;[66] (b) information relating to a specific individual such as income or work performance record, medical history, income, purchases and spending habits, criminal record, personal bank statements or itemised telephone bills; or (c) an event or transaction which focuses on an individual such as the minutes of a disciplinary or tribunal hearing.

66 As "personal data" could encompass a whole range of characteristics, this should be borne in mind when contemplating exclusions from the definition of "personal data". MICA has proposed key exceptions to include personal data cited in court documents, photographs of individuals taken for personal use and published, for example, on a blog or Facebook page, personal information collected for news reporting, medical emergencies, national security and research purposes. A further exception would be location-based marketing, where retailers broadcast promotional SMSs to consumers who are physically near their shops.

67 MICA is seeking views on whether to exclude the collection, use and disclosure of personal data solely for artistic or literary purposes, as in Canada.

68 The proposed legislation defines "personal data" as "information about an identified or identifiable individual; where individual means a natural person whether living or deceased".[67] The scope of the definition is very wide. It is not, however, feasible to contain a definitive list of "personal data" as this is context-specific and new types may be generated by technology such as IP addresses which can be linked to information about ownership or usage. However, the DPC may publish guidelines as to the type of personal data that may be regulated under

65 National registration identity card/foreign identity number.

66 These are unique attributes assigned to a person or information about an individual which can be used to identify him.

67 Reference is made to the definitions in Canada, the UK and OECD Guidelines.

the new laws. MICA's Public Consultation Paper, however, suggested that certain information should be excluded, including business contact information (*eg*, name, title, business address or telephone number of an employee of an organisation) and work product information.[68] Thus, businesses collecting, using, disclosing, transferring and storing business data would not be regulated by the new law.

69 In this connection, it is timely to consider whether to regulate employment data which was exempted from the definition in the Model Code for the reasons cited above. The proposed limited exception for the purpose of mergers and acquisitions and in establishing, managing and terminating an employment relationship has been noted above. On the other hand, the Malaysian Personal Data Protection Act 2010 gives rise to new rights and obligations in the context of the employer-employee relationship, apart from merger and acquisition transactions involving personnel issues and the discharge of certain professional services, to name a few.

70 Any data protection legislation has to consider whether "personal data" should encompass all data formats or only electronic data (*eg*, under the Singapore Model Code) and whether the definition of "personal data filing systems" should encompass both computer and manual processing of data (as in the EU, Hong Kong and Taiwan under its new Personal Data Protection Act passed in April 2010) or whether it should apply only to electronic data and exclude manual filing systems (*eg*, in Japan and under the Singapore Model Code). However, this will be of decreasing significance with much of the transfer of personal information involving electronic data. Manual filing systems are excluded from the Model Code for the practical reason that it will be difficult for manual filing systems to comply with the privacy principles relating to access and accuracy.[69]

71 The new legislative framework intends to cover all forms of personal data, including both electronic and non-electronic forms of personal data, in order to better protect consumer interests as much data is still being collected, processed and stored using non-electronic means, such as lucky draws.

---

68 Section 2 of British Columbia's Personal Information Protection Act defines "work product information" as "information prepared or collected by an individual/group of individuals as a part of the individual's/group's responsibilities or activities related to the individual's/group's employment or business, but does not include personal data about an individual who did not prepare or collect the personal data".

69 National Internet Advisory Committee Legal Subcommittee, *Report on a Model Data Protection Code for the Private Sector* (2002) at para 6.1.6.

(1) Sensitive personal data

72 The Singapore Minister referred to the protection of sensitive data when announcing the introduction of the Consumer Data Protection Bill. The proposed legislation should prohibit the collection of sensitive data unless consumers consent, or if it is required by law or in other special circumstances such as those relating to public safety or health services provision. Given the likely harm resulting from the mishandling of sensitive data, the new law should consider special provisions to deal with such data. While recognising that certain types of personal data require higher levels of protection than others, MICA's Public Consultation Paper did not make any specific recommendation on protection of sensitive personal data, probably due to the fact that the new legislation will take a minimal baseline approach. This is in sharp contrast to the stringent protection of sensitive data in other key jurisdictions. Article 8 of the EU Directive places special restrictions on the processing of personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and health or sex life (subject to a few exceptions) and biometric personal data (unique physical characteristics that can be used to identify a person, *eg*, behavioural characteristics such as typewriting and handwriting patterns, retina and iris patterns, and voice). There is no provision in the Model Code specifying categories of sensitive data. Neither is there any provision dealing with automated processing which poses risks to an individual's rights and freedom which is provided in the EU Directive. Article 15 gives an individual the right not to be subject to a decision based on such automatic processing except pursuant to a contract or authorised by law. Aligning the new law with Articles 8 and 15 will assist Singapore in being designated "adequate" under the EU Directive and facilitate uninterrupted data flows with EU Member States as well as strengthen the positioning of Singapore as a trade and business hub.

73 Hong Kong published a Consultation Document on the *Review of the Personal Data (Privacy) Ordinance* on 28 August 2009. The Hong Kong Privacy Commissioner for Personal Data, in his submissions on the Consultation Paper, suggested an extended definition of sensitive data to include data regarding an individual's race or ethnicity, political and religious beliefs and affiliations, physical and mental health and sexual preferences. The Consultation Paper had proposed that the definition should include only biometric data at this stage. After a lengthy review process, the Government introduced the Personal Data (Privacy) (Amendment) Bill 2011 on 13 July 2011.

74 The Malaysian Personal Data Protection Act 2010 regards sensitive personal data which requires the explicit consent of the data

subject to include medical history, religious beliefs, political opinions and the commission or alleged commission of any offence.

(2) Personal data of deceased individuals

75 Protection of such data raises issues as to the extent of protection required and the administrative difficulties involved in obtaining consent. For similar reasons, the UK Data Protection Act covers personal data relating only to living individuals. Canada's Personal Information Protection and Electronic Documents Act[70] ("PIPEDA") extends to the personal data of persons who have been dead for less than 20 years. MICA has proposed the latter approach in relation to the safeguarding and disclosure of the personal data of deceased individuals.

(3) Existing data

76 Under the new laws, consent will be deemed to have been given for personal data collected prior to the enactment of the Act provided it is restricted to reasonable existing uses, taking into account the nature of the business. Fresh consent is needed if the existing data is to be used for a new or different purpose.

I. Obligations on organisations

77 Organisations which collect and hold personal data should register with the enforcement authority or regulator which in Singapore will be the DPC. If an organisation does not meet its obligations, individuals may complain to the DPC. All organisations should be required to implement procedures to minimise risks, adopt good management practices and educate employees on data protection and to notify the regulator of the security measures taken to protect personal information.[71] It is proposed that the organisation remains accountable under the new Act notwithstanding designating one or more officers for the purpose of ensuring compliance with the new law.

78 Organisations should observe general principles regarding the collection and use of personal data. They are required to inform consumers of the purposes for which their personal data will be used or disclosed and obtain their consent. The consent can be withdrawn at any time, following which all data must be deleted from the data base or anonymised. For example, organisations conducting lucky draws should not ask for irrelevant information such as a person's salary or marital

70 SC 2000, c 5.

71 This is the position under the EU Directive and the UK Data Protection Act 1998 (c 29).

status. They should specify how they are going to use the information at the point of collection and cannot use the information for purposes beyond what they have obtained consent for, nor disclose or sell the personal information without prior consent.

79 Organisations should be required to make written declarations to the regulatory authority. Employees and agents will be bound to observe the terms of the declaration. The declaration should describe whether data is to be disclosed to third parties and transferred to another country. As data is to be used only for specific purposes, organisations should set procedures and promote data privacy practices and appoint officers/committees to assess, monitor and review data privacy measures in existing and new computer applications. Computerised records should be made available upon request. In this regard, guidelines and procedures should be provided by the regulatory authority.

J. National do-not-call registry

80 This is a key feature in the new framework to supplement data protection laws and is a direct response to the rampant use of personal contact information for unsolicited marketing purposes. It allows individuals[72] in Singapore to call to register their Singapore telephone numbers with the national do-not-call ("DNC") registry operator ("DNC Operator") to "opt-out" of unsolicited telemarketing calls, SMS, MMS messages and faxes from all organisations in Singapore. This obviates the need to register with every organisation. The registered numbers will remain on the registry until withdrawn by the owner. Telemarketers will be required by law to check the national DNC registry, maintained by MICA, no longer than one month before making telemarketing telephone calls or sending faxes, SMS or MMS messages to the numbers registered, unless the individual has given his explicit consent. Annual fees will be charged for checking the DNC registry for blocked numbers. Marketers will not be allowed, either directly or indirectly through outsourcing to a telecom service operator or call centre outside Singapore, to make unsolicited calls or send faxes or messages to blocked numbers. Both the company outsourcing the marketing function and the company providing the service are required to set up an account with the DNC Operator. However, registration of telephone numbers only blocks marketing messages[73] so that other

72 Ministry of Information, Communications and the Arts is proposing to include business phone numbers as telemarketing messages may be disruptive and unproductive.

73 One of the purposes is to (a) offer to supply, advertise or promote goods or services; or (b) advertise or promote the suppliers or prospective suppliers of goods

(*cont'd on the next page*)

messages may still be received. Examples given are messages from charitable organisations promoting volunteerism or electoral/political messages from political parties.[74]

81 Notwithstanding the compliance costs that may be incurred, MICA stated that the DNC registry may benefit telemarketers by effectively targeting consumers who are genuinely interested in receiving information on the products and services. In this way, telemarketing can be used as a credible marketing medium. Furthermore, in sending out messages to unregistered numbers, the telemarketer must ensure that the originating telephone number can be detected and displayed and it cannot make use of blocked or unlisted numbers.

82 However, e-mails for this purpose are excluded from the new law. As MICA's Public Consultation Paper explained, unsolicited e-mails can be blocked through e-mail filters and are less of a nuisance to delete when compared to telephone calls, SMS and fax messages which are more difficult to filter off.[75] However, it is common experience to find that one cannot filter off all spam messages as new spam messages continue to flood in-boxes. This is notwithstanding the Spam Control Act[76] which implements an "opt-out" regime with a right to unsubscribe from unsolicited e-mail messages. However, the Act does not criminalise spamming and the affected party must sue the spammer personally and claim injunctive relief, compensatory damages or statutory damages which may be up to $1m. Furthermore, most e-mails emanate from overseas and raise huge enforcement problems.

83 It is recognised that the DNC registry is not completely aligned with the Spam Control Act, which applies to unsolicited commercial electronic messages sent in bulk. These have to comply with certain requirements such as the labelling of messages with an <ADV> tag and the provision of an unsubscribe option. With the establishment of the DNC registry, marketing messages can only be sent to unregistered numbers or where the individual has expressly consented. The Spam Act will still apply if they are unsolicited commercial electronic messages sent in bulk. Where an individual has registered his number with the DNC registry but has consented to receiving marketing messages from an organisation, MICA is proposing that his request to unsubscribe from receiving bulk spam messages should not be treated as

and services; or (c) advertisements for land or interests in land or business investment opportunities ((c) adopts the position in Australia and Hong Kong).

74 Ministry of Information, Communications and the Arts, Public Consultation Paper: *Framework details for the Establishment of a national do-not-call Registry* (31 October 2011).

75 Ministry of Information, Communications and the Arts, Public Consultation Paper: *Proposed Consumer Data Protection Regime for Singapore* at para 5.5.

76 Cap 311A, 2008 Rev Ed.

a withdrawal of consent to receiving marketing messages under data protection law.

84 Does the law extend to calls or text messages from service providers with an existing business relationship with consumers such as banks or financial planners? These should be regulated if the purpose behind the national DNC registry is not to be undermined. MICA is proposing that existing business relationships between an organisation and a customer should not be exempted. Customers must give explicit consent to receiving marketing messages, unless the message relates to an existing product or service provided to the customer. Thus, a service provider, such as a bank, cannot call customers for telemarketing purposes if they have listed their numbers in the registry, unless they have given consent to be contacted. Those in doubt should call the bank to withdraw any consent which might have been given in the past. However, a bank can still contact customers for matters related to services that are not marketing in nature, such as verifying purchases on an existing credit card.

85 Canada's policy allows calls to be made to customers for up to 18 months after a sales transaction. However, there are practical problems in enforcing the law in relation to telemarketing calls originating from overseas call centres, particularly from unknown numbers. Many companies outsource their calls, for example, to survey companies.

86 In order to facilitate compliance but without increasing costs, MICA is exploring a free online number look-up service for SME firms that do not telemarket frequently but may need to make occasional calls. The Ministry has also proposed that numbers registered at the DNC registry be removed from marketers' contact lists through a "filtering" process done by the registry, funded by the Government and with the subscription fees paid by marketers.

87 The DNC registry is reported to have been highly successful in the US due to stringent enforcement. In a prominent case in 2009, the country's largest telecoms operator, Comcast Corp, was fined US$900,000 (at US$1 *per* call) for allowing its telemarketers to call customers on the list.[77]

88 Under the new law, an organisation in Singapore will be in breach for sending a marketing message to a telephone number listed in the DNC registry or without first checking whether the number is registered or where it is allowed to download the list of registered telephone numbers, it misuses the numbers obtained from the registry.

77 *The Straits Times* (16 September 2011).

Penalties of up to a maximum of $1m against telemarketers who infringe the law should be a great deterrent if stringently enforced by the new DPC which will oversee the DNC registry. Where infringements are non-malicious and affect few consumers, the DPC may provide for a penalty of up to S$1,000 *per* telephone number contacted. Registered consumers who still receive unsolicited calls and spam text messages have a right to complain to the DPC which will have the power to investigate such complaints and take enforcement actions. The DPC's decisions may be appealed against but no civil redress is available as contraventions are unlikely to cause substantial damage to individuals.

K. Wording

89 Consistent with the international drafting style evident in, for example, the Vienna Convention on the International Sale of Goods, the new Act should be written in layperson's language that is easy for both businesses and customers to understand. The Model Code is drafted with so many exemptions that it is complex and difficult to understand, even though it is general and flexible enough to be applied across sectors.

L. Technology and globalisation

90 The new legislation should keep abreast with technological developments and rapid globalisation. It must be technology neutral so as to be applicable across sectors or in the context of new technologies. An ongoing debate is whether IP addresses should be regarded as personal data. Without taking into consideration such technological developments, the new law would already be out-of-date. Hence, the statutory provisions have to deal adequately with globalisation and the need to protect information as it flows across borders. In this respect, the new laws should address the rampant use of "cookies" which are dealt with in the EU Directive on "cookies" and in the proposed US "Do-Not-Track" legislation. However, there is the problem of jurisdiction over foreign websites. The Singapore approach is unlikely to be as stringent, bearing in mind the need to keep business costs manageable. Hence, it will give the flexibility to "opt-in" to higher standards based on industry demand.

M. Transborder data flows

91 While consumers may be assured that their personal data will be protected when collected and used in Singapore, they must be assured of similar standards of protection once their data is transferred outside Singapore in cases such as airline reservations, credit card transactions

and electronic funds transfers and particularly in light of market developments such as cloud computing.

92 The principle of "fair and lawful"[78] processing requires organisations to inform individuals about disclosures of their personal data to third parties overseas, how such information is sent and what contracts or safeguards are in place. Organisations should have full control over how personal data is used, ensure data security and accuracy and remain liable for any breaches.

93 With internationalisation, business outsourcing and instantaneous transfers of information through the Internet, it is timely to look beyond Singapore's domestic needs to international norms and requirements and regulate the transborder transfers of data.[79] This will directly align the new legislation with the EU Directive and the laws of other trading partners. Article 25 of the EU Directive prohibits the transfer of personal data outside the EU unless the receiving country, in the opinion of the European Commission, provides "adequate levels of protection" for personal data according to EU standards or if one of several very limited exceptions applies[80] or if the data exporter has taken steps to ensure to the satisfaction of the European local data protection authorities that the data will be adequately protected after it leaves the EU.[81] These are intended to prevent data processing operations occurring outside of the EU which are not subject to equivalent data protection laws, thus undermining the EU Directive.

94 Furthermore, it is the prevalent view that under Art 25 of the EU Directive, a country which does not ensure an "adequate level"[82] of protection by reason of its domestic law or of the international commitments it has entered into, when exporting personal data, may be considered by the EU as having inadequate levels of protection. Considering that the EU is Singapore's second top trading partner in 2010, the new laws should also restrict the onward transfers of personal

78 "Fair" means in a way that is reasonably expected by the individual (data subject).

79 A transfer is not the same thing as the transit of data through a country *en route* to its destination.

80 The exceptions are: (a) unambiguous consent from the data subject; (b) the transfer is necessary for the performance of a contract; (c) the transfer is necessary to protect the vital interests of the data subject; (d) the transfer is in the public interest; (e) the transfer is made from a public register; or (f) the transfer of anonymised data if it is impossible to determine the identity of the data subject.

81 Such as where (a) the recipient is a US safe-harbor-certified company (applies only to personal data about European data subjects transmitted between the US and EU but not beyond it); (b) where the recipient arranges specific data protection safeguards by means of contract clauses or binding corporate rules; or (c) where the recipient uses the EU Commission-approved model contractual clauses.

82 The "adequacy requirements" on a country-by-country basis have been relaxed by the European Commission on a company-by-company basis.

data to ensure that such data enjoys "adequate levels of protection".[83] This is particularly so since Singapore is currently not considered to be in the same league as the European Economic Area ("EEA") countries.[84] Transferring data from any EU Member State to any of these countries would be similar to transmitting data within the EU Member States. As at February 2011, the European Commission has recognised Andorra, Argentina, Faeroe Islands, Guernsey, Israel, Jersey, the Isle of Man, Switzerland, Canada for certain types of information and the US Department of Commerce Safe Harbor Privacy Principles, as providing adequate protection. The European Commission has also approved transfers of advance airline passenger data to the US and Australia.

95 Two recent enactments on the regulation of cross-border data flows are instructive. The New Zealand Privacy (Cross-border Information) Amendment Act 2010 addresses more adequately the cross-border transfer of personal information. The Commissioner is given the power to prohibit the transfer of personal information outside New Zealand if the data is transferred from a country to New Zealand and is likely to be transferred to another country that has inferior data protection safeguards as those in New Zealand or if the transfer is likely to breach basic principles of national application as set out in Pt 2 of the OECD Guidelines and the new schedule in the Privacy Act. Non-compliance with the transfer prohibition notice is punishable by summary conviction to a fine of up to $10,000. Transfer prohibition notices can be appealed and set aside or may be varied or cancelled by the Commissioner. The Malaysian Personal Data Protection Act 2010 also prohibits the transfer of personal data out of Malaysia, unless the country has been gazetted by the Minister of Information, Communication and Culture, or unless the data subject has consented to the transfer or where the transfer is necessary for the performance of a contract between the parties. APEC has proposed a cross-border privacy rules system.

96 In this regard, the Model Code is said to have "severe shortcomings in terms of scope, processes and enforcement mechanisms"[85] and is therefore unlikely to meet the EU's "adequacy" requirements. These should be noted in the drafting of the new

---

83 Vili Lehdonvirta, "European Union Data Protection Directive: Adequacy of Data Protection In Singapore" [2004] Sing JLS 511 observed that there is still some way to go before Singapore can claim to provide an adequate level of protection.

84 http://www.ico.gov.uk (accessed 21 April 2011). These are currently Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden.

85 Vili Lehdonvirta, "European Union Data Protection Directive: Adequacy of Data Protection in Singapore" [2004] Sing JLS 511.

legislation. However, Singapore's proposed approach to the transfer of data outside her jurisdiction falls far short of EU standards. The proposal is to adopt a "principle based" approach, as opposed to a prescriptive approach requiring adequacy rulings for foreign regimes or approving binding corporate rules. Under the proposed law, the onus will be on the company transferring data outside Singapore to take appropriate measures to protect such personal data as it is considered to have control over the data. What principles will be adopted remains to be seen.[86]

N. Extra-territorial reach

97 With the increasing processing of data on a global scale, Singapore should consider legislation in the broader international context and having extra-territorial reach so that data privacy laws may be enforced across borders. The DPC should be empowered to investigate data privacy violations committed by local companies overseas and to co-operate with investigators in other jurisdictions, for example, through information sharing. The power of the authorities to share information would depend on the memoranda of understanding between the respective countries, the consent by the complainant or under an exception to the general rule of non-disclosure. Such an approach is apparent in the Canadian, Australian and New Zealand data protection legislation.[87]

O. Regulatory authority and enforcement powers

98 The proposed legislation should provide for a government regulatory authority with advisory, supervisory and enforcement powers. It should not be bogged down by enforcement alone but also be responsible for developing policy and public education and for international liaison in data protection and data transfer.

99 The regulator should provide guidance, monitor and supervise compliance with data protection requirements, ensure that organisations are carrying out their obligations and that individuals' rights are upheld and conduct investigations into alleged breaches with power to carry out criminal investigations and prosecutions, search premises and seize evidence and call upon public officers for assistance.

86 Ministry of Information, Communications and the Arts, Public Consultation Paper: *Proposed Consumer Data Protection Regime for Singapore* at para 3.61.

87 New Zealand Privacy (Cross-border Information) Amendment Act 2010.

100 The regulator should keep a register of persons holding personal data. It should be open to public access[88] in accordance with the OECD Guidelines to enable data subjects to know what data is held about them, by whom and for what purpose. Organisations should be required to notify the supervisory authority of the details of automatic personal data systems before processing.[89] A register of such notifications should be kept by the regulatory authority.

101 As in other jurisdictions, regulatory authorities are part and parcel of the data protection framework. Hong Kong established the Office of the Privacy Commissioner for Personal Data and conferred on it significant powers. Malaysia's Personal Data Protection Act 2010 also provides for advisory, regulatory and enforcement bodies, the first to be set up being the Personal Data Protection Commissioner. The Data Protection Fund, Personal Data Protection Advisory Committee and Appeal Tribunal may also be set up under the Act.

102 The EU Directive requires each Member State to set up a Supervisory Authority or Data Protection Authority ("DPA"). The UK Data Protection Act gives the Information Commissioner powers to assess whether or not organisations are complying with the Act; require specified information within a fixed time frame; serve enforcement and "stop now" orders where there has been a breach of the Act; require organisations to remedy any non-compliance; prosecute those committing criminal offences under the Act; and conduct audits to assess whether the processing of data follows good practice and report to Parliament on data protection issues of concern. Since 6 April 2010, the Information Commissioner is empowered to impose monetary penalties of up to £500,000 on data controllers that knowingly or recklessly commit serious contraventions of the data protection principles. Furthermore, organisations which do not have adequate data control systems in place to guarantee the security of all personal data from collection to destruction could face fines of up to £5,000.

103 Recently, Google was fined one of the largest fines of €100,000 by the French data protection authority for unfair collection of data including e-mail exchanges and passwords through Google cars photographing streets to enhance Google maps.

104 The EU Article 29 Working Party ("WP 173")[90] has suggested a new provision requiring data controllers to implement appropriate and

88 EU Directive Art 21.

89 EU Directive Arts 18 and 19.

90 Set up under Art 29 of the EU Directive. It is an independent European advisory body on data protection and privacy. Opinion 3/2010 on the principle of accountability was adopted on 13 July 2010 at para 74.

effective measures to ensure that the principles and obligations of the EU Directive are complied with and to demonstrate this upon request.

105 Singapore should consider imposing criminal or civil penalties or both and providing private rights of action. Currently, the sectoral statutes typically impose penalties on public bodies and organisations for infringements but do not confer private rights of action or direct remedies that are available under data protection laws elsewhere. Only indirect protection through limited private action is available under the common law.

106 The experience of other data protection legal frameworks is useful. Under the EU Directive, the DPA has enforcement powers such as imposing fines on non-filers and the data subject is given a private right of action.

107 Although perceived to be weak penalties, the Hong Kong Ordinance provides for fines of between HK$5,001 and HK$10,000. Data users who contravene an enforcement notice served on them will face imprisonment for two years and a fine of between HK$25,000 and HK$50,000. For continuing contraventions, the daily penalty is HK$1,000. In addition, an individual who suffers damage as a result of a data user's contravention of the Ordinance is entitled to compensation for that damage, including injury to feelings. The Personal Data (Privacy) (Amendment) Bill 2011 creates a new offence of disclosing personal data without consent with intent to obtain monetary gain, cause financial loss or psychological harm to the data subject. The penalties will be a fine of HK$1m and imprisonment for five years. There is also a new provision empowering the Privacy Commissioner to provide legal assistance to data subjects who intend to seek compensation from data users under the Personal Data (Privacy) Ordinance. Assistance will be rendered only where the claim raises a question of principle or is complex in nature.

108 The Malaysian Personal Data Protection Act 2010 imposes criminal sanctions such as imprisonment or fine or both on data users for breach of the statutory provisions.

109 The Australian Law Reform Commission, in its report *For your information: Australian Privacy Law and Practice (ALRC 108)*, has recommended strengthening the enforcement powers of the Privacy Commissioner, including imposing a civil penalty where there is a serious or repeated interference with the privacy of an individual and enforcing undertakings to ensure compliance with the Act.

110 The Singapore DPC which will be set up to enforce the Act will use a complaints-based approach rather than a more stringent audit-based regime. The DPC will investigate cases of non-compliance with the data protection rules rather than regularly audit organisations or require regular self-audit reports to be submitted. MICA's Public Consultation Paper explained that the rationale for this approach is to keep business compliance costs manageable, reduce resources for administering the new regime and focus on more significant data breaches.[91] The Singapore approach is surprising, given the increasing powers sought by data regulators elsewhere. On the issue of enforcement, the penalty regime is intended to secure ongoing compliance while at the same time provide sufficient deterrence. The penalty regime is a tiered one that will enable the DPC to enforce remedies commensurate with the seriousness of the violation. The DPC has powers to issue orders for an organisation to rectify non-compliance and to pay a financial penalty not exceeding $1m. Such financial penalty is separate from any orders that might have been made. An appeal against the DPC's decision may be brought to an independent Appeals Board whose decision may be brought to court on appeal or for review. Individuals may also separately seek redress by civil proceedings in court. Apart from investigatory and enforcement roles, the DPC will focus on educating businesses and the public on proper data protection processes. The DPC's powers to investigate and impose penalties should be for both past and continuing infringements.

111 This is seen in the Hong Kong Personal Data (Privacy) (Amendment) Bill 2011 which extends the Commissioner's power to issue an enforcement notice where a data user is contravening or has contravened the Personal Data (Privacy) Ordinance[92] whether or not the contravention has ceased or is likely to be repeated. In the recent *Octopus* investigation involving the use of personal data in direct marketing, an enforcement notice could not be issued since *Octopus* had rectified its practices by the time of the investigation. The Hong Kong Bill changes this.

112 It is envisaged that for many cases, the DPC in Singapore will focus on early resolution of complaints by facilitating discussions between the parties or referring them to mediation.

113 MICA expects the majority of contraventions to be minor or non-malicious and which can be adequately addressed by the issuance of orders for corrective action. However, violations that cause significant harm to individuals would warrant stiffer penalties. In such cases,

91 Ministry of Information, Communications and the Arts, Public Consultation Paper: *Proposed Consumer Data Protection Regime for Singapore* at para 3.5.

92 1995 (Cap 486).

financial penalties could be imposed on top of any orders for corrective action.

114 The DPC can also impose criminal penalties on those who obstruct the DPC in the performance of its duties or powers under the Act, knowingly or recklessly make false statements, knowingly mislead or attempt to mislead the DPC or fail to comply with the DPC's orders made under the Act.

115 The DPC can also initiate investigations, whether a complaint is received or not, into an organisation's alleged non-compliance. It may also refuse to conduct or continue its investigations, *eg*, when the request is frivolous or vexatious, is not made in good faith, the circumstances warrant a refusal or suspension, when any party has commenced proceedings or when the parties have mutually agreed to settle the matter.

116 Since the new Act is expected to operate concurrently with other sectoral regulations, it would be desirable for the organisation to be subject to the investigative and enforcement actions of one regulator. The Act should therefore provide the DPC with powers to refer an incident to another regulatory agency.

117 The DPC will have powers to issue regulations, codes of practice and guidelines to supplement the Act. For example, the guidelines should explain what is personal data, what constitutes consent and the fee structure for requests to access personal data.

P. Data breach notification

118 It is worth considering whether there should be a specific data breach notification provision that requires organisations to have data breach management procedures and to notify the regulator and the affected individual of any data privacy breach or leakage of personal information. This will prepare organisations to better handle data breaches and preserve customer confidence. The introduction of a mandatory data breach notification requirement with civil penalties for failure to report breaches was recommended by the Australian Law Reform Commission ("ALRC 108"). The report, published on 11 August 2008 and containing about 2,700 pages, recommends sweeping reforms to Australian privacy law after a substantial review of local laws as well as trends in other jurisdictions, particularly in the US and Europe. Data breach notification laws have also emerged in countries such as India, Chile, Mexico and Brazil. From 1 July 2011 onwards, it becomes compulsory for providers of electronic communications services

("ECS")[93] in the EU to report data security breaches,[94] non-compliance with which carries criminal penalties. The EU has indicated its intention to extend the compulsory breach notifications to all sectors as part of the imminent reforms to the EU Data Protection Directive.

119 It is apparent that laws that require frequent notification to data protection regulators and even customers of data security breaches is an onerous requirement that may put a disproportionate burden on businesses and increase costs. Not every breach should be notified, only substantial breaches which are harmful to individuals.

Q. Data user return scheme

120 The Hong Kong Privacy Commissioner for Personal Data has sought consultation on the launching of a data user return scheme ("DURS") pursuant to Pt IV of the Personal Data (Privacy) Ordinance. With increasing awareness of data privacy rights, it is timely to ensure that organisations have responsible data policies and practices and are open and transparent about them through the introduction of the DURS. The returns will be used to maintain a register which will be made available for public inspection. The DURS is expected to be rolled out in phases and will cover the following categories of data users: the public sector, banking industry, telecommunications industry, insurance industry and organisations with a large database of members, *eg*, customer loyalty schemes. The consultation document indicated the Commissioner's view that the requirement of the annual return "will ensure data users are continuously reminded of their obligations and enables them to review and maintain high standards in personal data privacy protection throughout the organisation". Experience shows that after the introduction of a DURS in the EU, many corporations took personal data protection more seriously and appointed official personal data protection officers to ensure internal compliance and education.

R. Implementation

121 The new Act should be brought into force after giving businesses adequate time to implement compliance procedures. Guidelines should be provided to explain how the Act works, along with ongoing guidance and education. MICA proposed to adopt a single "sunrise" period of between one to two years for all provisions in the Act in order to facilitate compliance and administration. Guidelines on

93 Including cloud computing providers, internet service providers and telecommunications service providers.

94 European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011.

compliance will be published and awareness-building activities conducted.

VI. Implications on information management

122 With the introduction of specific data protection laws, organisations should consider their own data privacy practices and what processes need to be changed in readiness for the implementation of the new laws. Organisations[95] should ensure that all personal information is collected, processed and used "fairly and lawfully". They have to implement company compliance solutions such as privacy policies and procedures for managing data. Corporate privacy officers will be required to revise their privacy policies to ensure compliance with privacy rules in Singapore and in countries where they do business. These will ensure the free flow of data to Singapore and raise public confidence in the security and confidentiality of personal data held on computers.

123 Corporate policies should reflect fair information principles and comply with minimum standards for collecting and processing personal data. Businesses should also implement company-wide codes of conduct (such as those used by DaimlerChrysler[96]), security measures, data breach management, standard data protection contractual provisions prior to transferring to third countries, and last but not least, education and training programmes to inculcate data privacy consciousness in employees. Data protection laws will increase levels of awareness and compliance with data protection obligations amongst organisations and increase awareness about data protection rights among the public.

124 Since an organisation will be fully responsible for the actions of data processors to whom it subcontracts or outsources its services, it should adopt contractual or other means to prevent any data transferred to the data processor from being kept longer than is necessary for the processing and to prevent unauthorised or accidental access, processing, deletion, loss or use of the data transferred.

125 The transitional provisions in the new Act should help organisations adjust to the new regime. They include a "sunrise" period of two years between the enactment of the new law and the time it takes

95 These will also include security companies and management corporations of commercial buildings and private residential condominiums.

96 http://www.mercedes-benz.com.cn/content/media_library/china/mpc_china/OTHERS/Code_of_conduct.object-Single-MEDIA.tmp/COC_ITR_englisch.pdf (accessed 30 November 2011).

effect and deemed consent for existing uses of data so long as such uses are reasonable.

126 To what extent will compliance costs increase? Although data protection may affect management and administrative duties and business costs, studies on this have been inconclusive. Several members of the NIAC Legal Subcommittee expressed the view that the additional compliance costs would be minimal for private sector e-commerce organisations since the global nature of e-commerce already requires such organisations to comply with statutory data protection regimes in various industrialised countries.[97]

127 It is of some consolation to organisations that MICA's Public Consultation Paper stated that the key objective of the new data protection framework is to keep compliance costs manageable for businesses, especially SMEs. There would be a baseline law to ensure all private sector organisations comply with basic data protection requirements. Furthermore, the complaints-based approach rather than a requirement for audit reports is intended to keep compliance costs manageable.[98]

128 However, MICA's Public Consultation Paper recognised that the national DNC registry may impose additional compliance costs on telemarketers but that this will be offset by the saving of resources by targeting consumers who are genuinely interested in the organisation's products and services. This will preserve the viability of telemarketing as a credible marketing medium.[99]

129 The overall implications of the proposed legislation appear to be positive. It will build up customer confidence, enhance merchant credibility and enable businesses to gain a competitive edge in the marketplace. As the NIAC Legal Subcommittee observed, "good data protection is good business".

---

97 See Moira Paterson, "Privacy Protection in Australia: The Need for an Effective Private Sector Regime" (1998) 26 Federal Law Review 371 and Robert W Hahn, "An Assessment of the Costs of Proposed Online Privacy Legislation, Report Prepared for the Association for Competitive Technology" (7 May 2010) <http://actonline.org/publications/files/010507Privacystudy.pdf> (accessed 7 March 2012). Both articles are cited by the National Internet Advisory Committee Legal Subcommittee in *Report on a Model Data Protection Code for the Private Sector, Report 7*.

98 Ministry of Information, Communications and the Arts, Public Consultation Paper: *Proposed Consumer Data Protection Regime for Singapore* at para 3.5.

99 Ministry of Information, Communications and the Arts, Public Consultation Paper: *Proposed Consumer Data Protection Regime for Singapore* at para 5.6.

VII. Conclusion

130 Singapore's proposed legal framework has to strike a good balance between legitimate interests in operating business efficiently and the rights of individuals to data privacy protection and trust. The new laws should not restrict free data flow. If the law is too restrictive, it might impede business management and operations. Local business interests should also be balanced with data privacy protection requirements of overseas economies. As the European Commission has acknowledged, the free flow of personal information is essential for the efficient conduct of almost any economic activity. In the context of our global economy and global network, free cross-border data flows can facilitate international commerce while protecting information privacy. If based on international standards, it will be easier for global companies to adapt to the local system without incurring heavy business costs.

131 The proposed laws should ensure that personal data is "fairly and lawfully" processed, accurate, up-to-date and not kept for longer than is necessary. Minimum standards for protecting personal data should be set, giving individuals the right of access to information that is stored about them, to challenge any inaccurate or irrelevant data and to have any inaccurate data corrected or deleted. To ensure compliance with data protection principles, it is necessary to establish an independent data regulator with advisory, supervisory and enforcement powers.

132 The advent of globalisation and technological advancements requires Singapore to plug into international norms and to keep abreast with current reforms on data protection laws. It is not too late for Singapore to legislate comprehensively on this dynamic area of the law, when other nations are already embarking on a review of their own laws such as the EU, UK, Hong Kong and Australia. Even the People's Republic of China has seen it fit to issue on 30 January 2011 the draft Information Security Technology – Guide of Personal Information Protection, the first comprehensive law on the handling and transfer of personal information. The EU Directive is considered to be "now outdated – in terms of both technology and modern regulatory approaches. Technology has moved on massively in the last 20 years. It is a 'Mainframe Directive'".[100] Hence, negotiations on a new EU instrument for data protection are expected to begin in early 2011. In the UK, views are being sought as to whether the current data

100 Richard Thomas, "Data Protection in the European Union – Promising Themes of Reform" (former UK Information Commissioner) <http://www.privacycommission.be/nl/static/pdf/seminarie-privacyrichtlijn/data_protection_in_the_eu_nl.pdf> (accessed 7 March 2012).

protection laws are working in the light of social and technological changes since the mid-1990s.[101] Hong Kong's Personal Data (Privacy) Ordinance is also currently under review by the Government. Even Australia's data protection laws, considered one of the most comprehensive frameworks in the Asia-Pacific, have been extensively reviewed by the Australian Law Reform Commission which made 295 recommendations for amendments.

133 Singapore's proposed legislation will certainly benefit from these updates and amendments which will enable it to keep pace with 21st century data protection issues, such as those reflective of advances in technology and more sophisticated ways of doing business that are brought about by globalisation.

134 However, it is left to be seen whether the balancing act of trying to keep business costs manageable while safeguarding consumer interests will be tilted against effective personal data protection. As the proposed laws stand, their overall objectives appear to be more pro-business rather than pro-consumer.

---

101 UK Ministry of Justice, "Call for Evidence on the Current Data Protection Legislative Framework" (6 July 2010) at para 20.