NATIONAL
INTERNET
ADVISORY
COMMITTEE

Report On A Model Data Protection Code For The Private Sector

Prepared by The National Internet Advisory Committee Legal Subcommittee

Contents

EXECUTIVE SUMMARY

REPORT

ANNEXES

APPENDIX

NATIONAL INTERNET ADVISORY COMMITTEE

Report On A Model Data Protection Code For The Private Sector

Prepared by The National Internet Advisory Committee Legal Subcommittee

Executive Summary

International trends

1.1 Most of the world's data protection laws are based around sets of (variously named) information privacy principles which formally derive largely from two sources: the OECD Guidelines (1980)[1] and the Council of Europe *Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data* [2].

1.2 The latest progeny of this legislative line is the European Union's *Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (95/46/EC)* ("EU Directive"). The EU Directive has influenced legislation in Québec, New Zealand, Taiwan, Hong Kong and elsewhere. The EU Directive is, in most respects, a consolidation of the data protection instruments of the 1980s (and thinking of the 1970s).

Significance of EU Directive to Singapore

2.1 Although Singapore is not an EU nation, the EU Directive may possibly have an impact on us in two ways:

- Article 25 of the EU Directive prohibits EU nations from transferring personal data to third countries which do not guarantee adequate protection of such data.

[1] OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*

[2] (Convention No 108), in force since 1985.

- It is arguable that the EU Directive also requires, in this third country, a restriction against onward transfers of data to fourth countries which do not guarantee adequate data protection.

2.2 Thus, there is not only the possibility that the flow of personal data from EU countries to Singapore may be impeded, but that countries which want to ensure the free flow of personal data from EU countries would enact data protection laws *and* include in them restrictions prohibiting the transfer of data to countries without adequate data protection schemes (the “flow-on effect”). This has already happened in some of our neighbouring countries[3].

2.3 The EU is Singapore's **third largest export market** after Malaysia and the US. This, and the "flow-on effect", means that the lack of an adequate data protection regime in Singapore may impede international trade and place Singapore businesses at a disadvantage in the global economy.

Governing cyberspace

3.1 International trends are not the only reason for the development of data protection schemes in Singapore. With the advent of the information age comes the potential for mischief on an unprecedented level, both in terms of nature and scale. Data protection regimes impose discipline over a new breed of technology practitioners, who are yet to be regulated by any code of ethical behaviour, but who wield tremendous power over consumers by virtue of their potential to control personal data. Such discipline bolsters the confidence of consumers in the integrity of the e-commerce (and m-commerce) market, thus encouraging the increased automation of transactions between businesses and their customers, as Singapore strives to become an info-communications hub in a fully networked world.[4]

[3] E.g. in Australia, Hong Kong and Taiwan

[4] See e.g. article in The Straits Times, 1st August 2001 entitled **Pay-by-phone Commerce Gets A Boost** which states: "Singapore is set to be one of the world's first in coming up with a common nationwide method of paying for goods and services with mobile phones."

Current position

4.1 While Singapore has both a strong common law tradition as well as appropriately structured statutory provisions to regulate the use of personal data, there is *fragmentation* of the laws, both with regard to their subject matter and to their administration. There is no general and comprehensive data protection law. Varying degrees of protection are accorded by a great number of statutory provisions providing for the confidentiality of information in the possession of government agencies. Certain sectors are also governed by the common law and self-regulatory codes. This is similar to the position taken by the US which has thus far avoided enacting general data protection laws.

Scope of report

5.1 The main thrust of this Report is to set out the Subcommittee's views on what constitutes "fair information principles". These principles find expression as the 11 DPPs in the Model Code.

5.2 However, as the adequacy of a data protection regime depends not only on the fair information principles it is founded on, but also on implementation issues (such as enforcement and compliance mechanisms), this Report also sets out very briefly some of the Subcommittee's views on what may constitute an appropriate data protection model for the Singapore private sector.

Summary of recommendations

6.1 The main recommendations of the Subcommittee are:

6.1.1 Effective protection of personal data is desirable in the Singapore private sector.

6.1.2 The data protection regime for the private sector should be founded on internationally recognised standards of data protection.

6.1.3 As an interim measure, voluntary data protection guidelines for the private sector (such as the Model Code) should be given official recognition and adherence invited on a voluntary basis. The exercise will have an educative and harmonising function and should facilitate the introduction of legislation, should Parliament decide in the future to legislate.

6.1.4 In the longer term, it remains to be seen whether a reliance on voluntary controls in the private sector would be completely effective or whether an appropriate degree of legislative intervention may be required. The full effect of a self-regulatory regime is yet to be felt by industry, consumers, and by society as a whole, and much would depend on their response to the regime and how it works out in practice.

6.1.5 The data protection regime should be concerned with "personal data" in the sense of any representation of data, true or not, factual or judgmental, relating to a living individual whose identity is either apparent from the data, or can be reasonably ascertained. All data that are capable of being read intelligibly should be covered. The regime should not merely cover "sensitive" or "intimate" data. However, the level of protection will depend on the sensitivity of the data.

6.1.6 At this stage, the data protection regime should apply only to the processing of data wholly or partly by automated means. For practical reasons, the regime should not at this stage apply to processing of data otherwise than by automatic means, even if such data form part of a filing system or are intended to form part of a filing system. It would be difficult for manual filing systems to comply with some of the principles (e.g. access and accuracy). But if manual data are subsequently converted to electronic form, the data processor will, from that point onwards, be required to comply with the Model Code.

6.1.7 The data protection principles should immediately apply to data in existence upon adoption of the Model Code. However, the following principles will only apply after a transition period of one year:

(i) **Principle 6 (Accuracy)** – i.e. there would be no breach of this principle during the transition period;

(ii) **Principle 9 (Access)** – i.e. the data user would not be required to provide a full copy of all data held at the time of the request, but would be entitled to first clean up the data by updating and removing irrelevant or dubious data. The data user would then be obliged to provide the data subject with a copy of all the remaining data.

6.1.8 The data protection regime should apply to any personal data *processed or controlled* in Singapore, regardless of whether the data controller is within Singapore.

6.1.9 The data protection regime should apply in favour of all data subjects, whether or not they are resident in Singapore. In particular, access and correction rights should not be restricted to Singapore residents.

6.1.10 The data protection regime should prevent organisations from transferring any data which would involve a loss of control over the data, to any recipient within or outside Singapore unless certain conditions are met.

6.1.11 Certain types of data, and certain types of data processing, may be exempted from the application from some or all of the data protection rules.

Report On A Model Data Protection Code For The Private Sector

Prepared by The National Internet Advisory Committee Legal Subcommittee

1. PREFACE

1.1 This is a report by the Legal Subcommittee of the National Internet Advisory Committee ("NIAC") on the *Private Sector Model Data Protection Code* ("Model Code").

1.2 The Model Code aims to strike a balance, in this information age, between the legitimate information needs of businesses, industries and institutions, on the one hand, and individuals' interests in the protection of their personal data, on the other.

1.3 The Model Code is modelled after the *Canadian Standards Association's Model Code for the Protection of Personal Information (CAN/CSA-Q830-96)* ("CSA Code"). The CSA Code has been approved as a National Standard of Canada by the Standards Council of Canada and is based on the Organisation for Economic Cooperation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD, Paris, 1981) ("OECD Guidelines").[5]

1.4 The Model Code establishes 11 basic Data Protection Principles ("DPPs") for private sector organisations that collect or use personal data. These 11 DPPs establish what is hoped will eventually serve as a national benchmark, across industries and across sectors, for the fair handling of personal data. Retailers (including e-tailers), direct marketers, financial institutions, telecommunications companies, product manufacturers, service providers, universities and hospitals are just some of the potential users of personal data with whom the Model Code has been drafted in mind.

[5] Further background information on the CSA and the CSA Code is set out at paragraphs 8.8 to 8.10, below.

1.5 The Model Code may be adopted wholesale. Alternatively, it may serve as a template upon which more industry-specific data protection rules may be based. In this regard, the Model Code has been designed to provide flexibility, allowing rules to be varied or stated in a different manner according to legitimate needs of each sector and in the context of its own environment.

1.6 The Model Code thus serves **two purposes**:

- It establishes minimum acceptable *standards* for data protection.
- It promotes the *harmonisation* of data protection rules among the various sectors, rendering the future establishment of any data protection regime an easier task.

2. MEMBERS OF THE NIAC LEGAL SUBCOMMITTEE[6]

2.1 The Model Code is the result of a collaborative effort by members serving in their personal capacities but who are drawn from key groups concerned with online data protection in Singapore. The 17-member Subcommittee that developed the Model Code includes representatives from:

- the government, including AGC, IDA, SBA and the Police
- the academia
- Small and Medium Enterprises (SMEs)
- private sector lawyers
- the media
- the health service industry
- the info-communications industry
- specialists in information technology

3. BACKGROUND OF REPORT

3.1 In 1999, the NIAC Legal Subcommittee proposed an *E-Commerce Code for the Protection of Personal Information and Communications of Consumers of Internet Commerce*. This Code has since been adopted by CaseTrust and incorporated into its Code of Practice as part of an accreditation scheme promoting good business practices among store-based and web-based retailers.

[6] *Annex 1* sets out the list of members of the Legal Subcommittee who worked on this Code

3.2 However, the drafting of the E-Commerce Code did not take into account the more recent *EU Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (95/46/EC)* ("EU Directive")[7]. The Chairman of the Legal Subcommittee, Mr Charles Lim, suggested to the NIAC that a more comprehensive code be drawn up taking into consideration the EU development. The NIAC thus assigned to the Legal Subcommittee the task of expanding the relevant portion of the E-Commerce Code into a Data Protection Code for Industry Self-Regulation in Singapore.

3.3 The first initiative taken by the Chairman of the Legal Subcommittee was to co-opt several new members, hailing from various backgrounds dealing with or concerned with data protection, to provide more views and feedback on the issue of data protection.

3.4 The Subcommittee met on four occasions (24 Feb 2001, 21 Apr 2001, 11 May 2001 and 26 May 2001) to discuss the draft Code. Numerous informal discussions were also conducted via email.

3.5 The development of data protection regimes globally has not gone unnoticed by the Singapore government. While work on the NIAC Model Code was ongoing, it was announced in Parliament[8] that the Ministry of Communications and Information Technology (MCIT) would spearhead an inter-agency task force to study general privacy issues, taking into account international developments. It was stated in Parliament that the inter-agency study would "*focus on the impact of e-commerce and Internet on data protection and privacy and will cover, among other things, financial information collected from e-commerce websites*".

3.6 While the work undertaken by the NIAC and the inter-agency task force may overlap to a certain degree, the efforts of both committees could effectively complement each other. [9]

[7] Effective 25 October 1998. The EU Directive is set out at *Appendix A*.

[8] By Deputy Prime Minister BG Lee Hsien Loong. See Parliamentary Debates, 22 Feb 2001 (at column 1431)

[9] An active interest in data protection issues by both the private and public sectors is conducive to the adoption of a co-regulatory scheme - See Part 6 on "Possible data protection models".

4. PRESENT DATA PROTECTION FRAMEWORK IN SINGAPORE

4.1 While Singapore has both a strong **common law** tradition[10] as well as appropriately structured **statutory provisions**[11] to regulate the use of personal data, there is *fragmentation* of the laws, both with regard to their subject matter and to their administration. There is no general and comprehensive data protection law. This is similar to the position taken by the US which has thus far avoided enacting general data protection laws.

4.2 Data protection provisions in Singapore also tend to take the "traditional" approach of regulating only the more common forms of "processing" (such as collection and disclosure). It may not have fully taken into consideration modern jurisprudence in the area of data protection which deals also with such issues as rights to access and correction, accuracy, and data security.

4.3 Thus, while Singapore laws protect personal data in certain sectors and even complements such protection with a host of other IT laws on a broad spectrum of issues, there is no *uniform* approach. Instead, varying degrees of data protection are accorded by a great number of statutory provisions providing for confidentiality of information in the possession of the government or particular sectors. A drawback with this sectoral approach is that it requires new legislation to be introduced with each development of new technology.

4.4 Aside from the legal framework, other, more pro-active, sectors have adopted varying degrees of security and confidentiality measures on a voluntary basis, in some cases reinforced by advisory codes of practice for their sector[12]. However, again, such initiatives may not provide a uniform, comprehensive, data protection regime[13].

[10] E.g. common law remedies for breach of confidence, copyright, defamation and negligence; law of contract on express or implied terms; public interest immunity; legal professional privilege.

[11] Covering such disparate topics as national security and census-taking, and such specialised topics as interception of communications and insider dealing. See *Annex 2* for a list of Singapore legislation touching on the confidentiality of personal data (compiled in 1999).

[12] E.g. the DMAS and NATAS Codes, and the NIAC's *E-Commerce Code for the Protection of Personal Information and Communications of Consumers of Internet Commerce*. As mentioned above, the NIAC E-Commerce Code had not taken into consideration the more recent developments in the EU.

[13] The usual inadequacy here is not in relation to the existence of comprehensive standards, but adequate compliance and redress mechanisms.

5. THE NEED FOR A HARMONISED, COMPREHENSIVE, DATA PROTECTION REGIME IN SINGAPORE

Governing cyberspace

5.1 Singapore in the 1990s, like most other industrialised countries, is characterised by a high level of technological development, and the increased automation of transactions between businesses and their customers. With the advent of the information age, however, comes the potential for mischief on an unprecedented level, both in terms of nature and scale.

5.2 Data protection regimes impose discipline over a new breed of technology practitioners, who are yet to be regulated by any code of ethical behaviour, but who have the potential to wield tremendous power over consumers by virtue of their control over personal data. Such discipline bolsters the confidence of consumers in the integrity of the e-commerce[14] market, thus encouraging the increased automation of transactions between businesses and their customers, as Singapore strives to reap the full benefits of the information age for the benefit of her citizens.

Growth of e-commerce

5.3 The potential danger posed by data protection issues on the growth of e-commerce was reiterated in the revised Explanatory Statement to the Privacy Amendment (Private Sector) Bill 2000 (Commonwealth of Australia)[15]:

> *"Surveys conducted in Australia and in other countries such as the United States have indicated that consumer confidence in electronic commerce depends largely on the level of protection afforded to their personal information. Consumers want some limitations imposed on the private sector in respect of personal information that may be collected. Also, consumers want stronger controls regarding how their personal information may be used after it is collected and to whom it may be disclosed outside the organisation. The Government acknowledges that if this issue is not adequately addressed, it has the potential to hamper the growth of electronic commerce."*

[14] Including m-commerce (mobile-commerce)

[15] At page 9

5.4 Similarly, in Victoria, Australia, public concerns about potential information privacy invasions have been a significant factor in prompting data protection initiatives[16].

5.5 A national survey in the US showed that 81% of the American public feel that consumers have "lost all control" over the way businesses collect and use their personal information.[17] A US Government report noted that "*if consumers feel that their personal information will be used or used in ways that differ from their original understanding, the commercial viability of the NII [National Information Infrastructure] could be jeopardised as consumers hesitate to use advanced communication networks*".

5.6 Members of the Legal Subcommittee felt that these statements accurately reflect some of the concerns faced by the Singapore public with respect to e-commerce.

Vulnerability of e-consumers

5.7 Modern technologies present ample opportunity for "scare-mongers" to generate high levels of paranoia, and hence undermine investments. Examples of applications that are especially exposed are electronic services delivery, Internet commerce, intelligent transportation systems, and anything that involves smart-cards or biometrics. Consumers need to be sure that personal data acquired from companies trading on the Internet are not misused, and that they will not be subjected to unsolicited or undesired advertising and marketing.

Impact of EU Directive on Singapore

5.8 Another aspect of the problem involves the continued transborder flow of personal data in support of global business activities. Private and public organisations wishing to participate in global trade need to continue to receive and communicate personal data on employees and consumers.

[16] The Treasurer and Minister for Multimedia, Alan Stockdale, in announcing the formation of Victoria's Data Protection Advisory Council, commented that the success of the proposed electronic service delivery system would largely depend on Victorians trusting that the information which they sent "would not be misused or accessed by unauthorised persons".

[17] The survey was conducted by Louis Harris and Associates, and is referred to in the Conference Report, "*Data Protection in the Global Society*" (1996). The report is available online at http://www.privacyexchange.org/iss/confpro/aicgsberlin.html

5.9 However, in 1998, the EU enacted legislation (the EU Directive) prohibiting the transfer of personal data by EU countries to a country that does not have an adequate data protection regime. The EU Directive does not purport to have extra-territorial jurisdiction, nonetheless it impacts Singapore in two ways:

- Article 25 of the EU Directive prohibits EU nations from transferring personal data to third countries that do not guarantee adequate protection of such data.

- It is arguable that the EU Directive also requires, in this third country, a restriction against onward transfers of data to fourth countries that do not guarantee adequate data protection.

5.10 Thus, there is not only the possibility that the flow of personal data from EU countries to Singapore may be impeded, but that countries wishing to ensure the free flow of personal data from EU countries would enact data protection laws *and* include in them restrictions prohibiting the transfer of data to countries without adequate data protection schemes (the “flow-on effect”). This has already happened in some of our neighbouring countries[18].

5.11 The EU is Singapore's **third largest export market** after Malaysia and the US.[19] This, and the "flow-on effect" if our other trading partners are required by the EU to block data transfers to Singapore, means that the lack of an adequate data protection regime applying to the private sector in Singapore may be an impediment to international trade. This may place Singapore businesses at a disadvantage in the global economy.

5.12 At this time, the Europeans are gradually clarifying how this provision (Article 25) is going to be enforced. But, while a comprehensive legislative scheme applying to both the public and private sectors (eg. HK, NZ, Canada) is clearly the easiest way to satisfy the EU Directive, Article 25 of the Directive is itself quite clear that a range of other options are available, including voluntary data protection codes applied by industries, or binding contractual clauses between the parties concerned in the data transfer.[20] Such measures may be considered

[18] E.g. in Australia, Hong Kong and Taiwan

[19] *Singapore-EU Trade and Investment Linkages: Two Years After the Launch of the Euro* (article by Economics Division of the MTI, dated 22 Feb 2001)

[20] Article 25(2) requires the level of protection afforded by a third country to be assessed in the light of *all the circumstances* surrounding a data transfer operation or set of such operations. Specific reference is made not only to rules of law but also to "professional rules and security measures which are complied with in that country." Thus, account may be taken of non-legal rules in force in the third country .

adequate *provided* they are effectively applied and offer sufficient safeguards concerning data subjects' rights, including rights of redress.[21] In July 2000, the European Commission approved the US' sectoral and self-regulatory approach to data protection known as the "Safe Harbour" arrangements[22].

5.13 It would appear that central to European concerns is the need to "*deliver a good level of compliance with the rules…A good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them.*"

5.14 At the very least, businesses that rely on the free transfer of personal data about European clients, consumers and competitors will have to assure the EU that their industry and professional codes, if such exist, are complied with. It appears that a statement of good intentions will not suffice. An international standard could simplify the process of determining adequacy within a highly complex and networked data processing environment.

Need for a harmonised regime

5.15 A proliferation of data protection regimes and practices is **confusing to consumers**. A wide variation of practices may even mislead some consumers. For example, some organisations' "privacy policies" posted on their websites are bland statements of good intention. Others are heavily influenced by the input of the corporate legal department, while yet others are simply difficult to find!

5.16 A diversity of data protection regimes also makes **monitoring and auditing by the relevant authorities** difficult.

5.17 Finally, just as inconsistencies between the laws of the various nations threaten commerce[23], so too do inconsistent regimes applied to different sectors within the same country. On the other hand, harmonised regimes translate into **lower operational costs for global businesses**, which only have to comply with a single set of requirements.

[21] The EU Working Party has issued guidance on industry self-regulation (Working Paper 12 – July 1998)

[22] The idea of the "Safe Harbour" is that US companies would voluntarily self-certify to adhere to a set of privacy principles worked out by the US Dept of Commerce and the Internal Market Directorate of the European Commission. These companies would then have a presumption of adequacy and they could continue to receive personal data from the EU.

[23] In the late 1960s, information privacy emerged as a serious social concern, resulting in many different laws being passed in the majority of advanced western nations in the period 1970-1985. This was the reason codification was undertaken, most notably by the OECD in 1980.

5.18 This is not to say that sectoral data protection regimes cannot play a part. Within the framework of a comprehensive data protection regime, sectoral legislation or codes may effectively complement a general regime by providing more detailed protection for certain categories of information, such as telecommunications, police files or consumer credit records.

Conclusion

5.19 Good data protection is good business. Certainly this is so in the long run. The Legal Subcommittee suggests that rewards will be reaped if private sector organisations are proactive in this area, co-operate in fostering a culture of protecting personal data in a harmonious fashion, and work together to ensure a vital, open domestic and international marketplace.

5.20 The Legal Subcommittee thus recommends that a uniform comprehensive data protection regime be introduced as part of a package of rules to facilitate trade and the growth of e-commerce generally.

6. POSSIBLE MODELS – ENFORCEMENT AND COMPLIANCE OPTIONS FOR A DATA PROTECTION REGIME

6.1 Codes are meaningless unless they are accompanied by a clear strategy to make them effective and ensure compliance[24]. Such issues go beyond the ambit of fair information principles (the "content" of a data protection regime) and are therefore technically outside the scope of the Subcommittee's study. Nonetheless, for the sake of completeness, the views of the Subcommittee on this issue are set out[25].

6.2 Five possible enforcement and compliance options were considered[26]:

- Comprehensive data protection laws
- Sectoral data protection laws
- Comprehensive codes of practice[27]

[24] It has been said that, "questions of content cannot be separated from questions of implementation" (Colin J. Bennett, *Prospects for an International Standard for the Protection of Personal Information: A Report of the Standards Council of Canada* at page 15).

[25] It must however be emphasised that an in-depth study of these issues was not attempted.

[26] It should be noted that this is not a rigorous classification, and there is no consensus on this classification. Other classifications exist.

- Sectoral codes of practice[28]
- Co-regulatory schemes

6.3 Depending on their application, these options can be complementary or contradictory. In several countries surveyed, a few of these options were used simultaneously in providing effective data protection. The relative advantages and disadvantages of each of these regulatory options are briefly set out in *Annex 3*.

Comprehensive regime

6.4 The Legal Subcommittee recognises that the overseas trend is clearly towards some form of omnibus or comprehensive data protection regime and suggests that the data protection regime for Singapore should similarly be comprehensive – geographically, jurisdictionally (subject to principles of international law), and sectorally – given that the information highway knows no boundaries. This also makes it easier to amend the law as circumstances change.

Self or co-regulation vs. prescriptive legislation

6.5 While many countries in Europe still adopt the traditional regulatory approach of prescriptive legislation (i.e. "command-and-control"), there is an emerging recognition that the adoption of legislation is not a panacea to all the ills in society. The trend now is to regulate less but regulate better. This is often attempted by utilising self or co-regulatory models[29].

6.6 The distinguishing feature of the co-regulatory model (over the self-regulatory model) is that the former acknowledges the important role of the government. The level of government involvement in a co-regulatory model spans a wide spectrum, from little control ("light touch") to more interventionist approaches.[30]

[27] E.g. the Canadian Standards Association (CSA)'s *Model Code for the Protection of Personal Information* and the Australian Privacy Commissioner's *National Principles for the Fair Handling of Personal Information.* A code of practice essentially means a set of data protection rules adopted by a significant number of members from the same profession or industry sector, the content of which has been developed and implemented by them. Like legislation, codes of practice may be comprehensive, applying to all data users, or sector or activity-based.

[28] These are more common than comprehensive codes, partly because they are easier to organise. Any attempt to develop a comprehensive data protection code of practice applying at least to all private sector data users will usually require some external catalyst, and for some independent body to take the initiative.

[29] E.g. Hong Kong, New Zealand, Australia, which provide flexibility in the application of the law by providing for recognition of industry and activity-based codes of practice.

[30] Examples of various co-regulatory data protection schemes in existence globally are set out at *Annex 3*.

Self-regulation

6.7 While a voluntary or self-regulatory regime (i.e. one that lacks mandatory statutory controls) has the attractive features of saving costs[31] and avoiding red tape, Canadian, Australian and United Kingdom law reform inquiries that have examined the matter have unanimously concluded that this approach provides inadequate protection to information privacy.[32] It has even been said that "in reality self regulation may equal no regulation and just provide a convenient tool to hold out and proclaim that something is being done about data protection".[33]

6.8 The dangers of relying on a self-regulatory regime are set out in Moira Paterson's[34] article on the Australian experience, *"Privacy Protection in Australia: The Need for an Effective Private Sector Regime*"[35]:

> *"A self-regulatory scheme will be effective only to the extent that businesses choose to become part of it. While there are a large number of businesses which are likely to do so, either because they are already committed to responsible privacy practices or because they hope to gain some commercial advantage from doing so, a large number of businesses were opposed to the implementation of legislation either on the basis of cost or because they felt that they should have an unfettered right to use personal data. It seems unduly optimistic to expect that all of them will participate in any scheme which provides more than mere window-dressing. Furthermore, those who might otherwise have been prepared to participate in an effective scheme may be deterred from doing so by the fact that they will be placed at a cost disadvantage in comparison to their less responsible competitors. … A purely voluntary scheme, without an effective oversight mechanism, is unlikely to generate the level of public confidence which is required to facilitate the growth of an embryonic electronic commerce industry and or to create and encourage the free flow of personal information into Australia."*

[31] At least to the government

[32] The UK Committee on Data Protection ("the Lindop Committee") considered that "a wholly voluntary approach would not suffice … [T]he public will, we believe, look … for an assurance that data protection can, in the last resort, be enforced." (*Report of the Committee on Data Protection, Cmnd.7772, 1979*)

[33] Tucker, Greg, "Frontiers of Information Privacy in Australia", (1992) Vol 3 No 1 *Journal of Law and Information Science*, p.66

[34] Senior Lecturer in Law, Monash University

[35] Federal Law Review, Vol. 26 No. 2 (1998) at page 8. The article is available at http://law.anu.edu.au/publications/flr/vol26no2/Patters.htm

Co-regulation

6.9 The Legal Subcommittee thinks that the logic of co-regulatory models is compelling for three reasons:

- This approach encourages **continuous and innovative self-improvement** by giving business greater flexibility, within a clear framework of societal expectations and requirements, rather than stopping at compliance with a set performance or standard. This puts to good use the entrepreneurial dynamism and informational advantages of the business sector and promotes active involvement of the business community in the policy-making process;

- This approach **reduces dependency on limited government resources** by making use of industry's knowledge and resources, thus reducing the expense of the government having to collect the information, develop this into regulations, and then monitor the effects, often without an appropriate level of industrial and process experience.

- The government is in the best position to promote **international co-operation and harmonisation** of self-regulatory schemes, and is more likely to be effective than any single sector in securing the **collective action of sectoral organisations**.

7. PROJECTED COMPLIANCE COSTS

7.1 On the important issue of compliance costs for the different models, Moira Paterson states[36]:

> *"The cost to an individual business of any privacy regime depends on what the regime requires in terms of registration and other book-keeping, the extent to which it requires substantial changes to that business's existing practices, such enforcement costs as are required to be funded by that business and the extent to which that business is required, or chooses, to comply with the regime. There is therefore **no logical reason why a statutory scheme should be any more costly than a voluntary one, assuming that they both offer adequate levels of privacy protection**."*

[36] *Ibid* at page 9

7.2 Several members of the Legal Subcommittee (from the private sector) expressed the view that the compliance costs arising from comprehensive legislation would ***not*** be a significant issue from a private sector ***e-commerce*** organisation's point of view. The reason was that the global nature of e-commerce businesses already requires most organisations which are involved in e-commerce activities to comply with one or more statutory data protection regimes in various industrialised countries. These members felt that if the Singapore statutory regime follows the common overseas model, the additional compliance costs would be minimal.

7.3 This view is consistent with Moira Paterson's statement in her same article that:

> *"Evidence from jurisdictions which have recently enacted private sector privacy laws suggest, however, that costs has not been a substantial problem. For example, the Australian Privacy Commissioner notes that private sector peak organisations representing banks, insurance companies and human resource specialists have all reported "minimal costs".[37] In fact there is evidence from Quebec which suggests that implementing data protection measures may more than pay for itself in terms of cost reduction or increased productivity that have resulted from improved information handling practices.[38]"*

7.4 On the other hand, Hahn, in a recent study[39], estimated that it may cost US companies up to US$36 billion to develop and implement the necessary information technology infrastructure to comply with online privacy legislation — sufficient to have a significant effect on business activity.

7.5 However, the Legal Subcommittee felt that Hahn's conclusions may not be reliable for the following reasons: **Firstly**, the study was based on draft information privacy legislation, not industry codes. **Secondly**, the study was funded and commissioned by the US Association for Competitive Technology. **Thirdly** and most significantly, members thought that some of the assumptions adopted by Hahn may not be correct. Hahn states his methodology at page 17:

[37] *Information Privacy in Australia: A National Scheme for Fair Information Practices in the Private Sector* (1997) (the Privacy Commissioner's Consultation Paper) at 47

[38] P Peladeau, "*Data Protection Saves Money*" Privacy Journal, June 1995, at 3-4.

[39] Robert W. Hahn, "*An Assessment of the Costs of Proposed Online Privacy Legislation*," report prepared for the Association for Competitive Technology, May 7, 2001, available online at *http://www.actonline.org/pubs/HahnStudy.pdf.*

> *"To obtain quantitative estimates of the cost, I requested that ACT collect estimates on the initial costs of modifying systems to allow a website to track the types of information discussed above. Then I estimated how many websites the proposed laws would affect. Finally, I multiplied the software cost by the number of affected sites to obtain an estimate of the industry-level cost to compliance."*

7.6 Hahn had thus estimated compliance costs by multiplying the assumed costs of software modification for one website by the number of websites likely to be affected by the draft US information privacy legislation. As such, the number of websites already equipped with online information privacy measures had not been discounted from the calculation. The difficulty of his task was even conceded by Hahn[40]:

> *"Quantifying the unit costs and the number of affected websites is a difficult task. First, since very few websites have needed software to track PII and its uses, little is known about much it would cost. Second, there are several estimates of the number of World Wide Web domains, but little data on how many of those are unique, U.S.-based, commercially viable sites, that collect and share PII, and would continue to do so if the proposed bills become law."*

7.7 In view of the apparent conflict of views and the lack of reliable data on the business costs of data protection compliance in Singapore, the Legal Subcommittee recommends that a comprehensive study on this important issue be conducted in the future.

Conclusion

7.8 In response to any argument that a data protection regime might be too costly to businesses, three points may be made:

- The **loss of one's reputation** as a responsible corporate citizen because of an information privacy scandal can be even more costly. Scandals, such as those involving the Lotus Marketplace product, the "P-Trak" database from Lexis-Nexis, the Pentium III chip, and more recently the "Doubleclick" software will continue to raise the profile of information privacy and temporarily force those data users whose practices have

[40] At page 16

been criticised to restore their reputations.

- Implementing data protection policy need not be a complicated process. Data protection could be a **component of** "**total quality management**" and indeed there are some interesting parallels between the fair information principles and the requirements of quality assurance.

- In some (but not all) cases, data protection principles are common-sense and may already be implemented as part of the responsible organisation's obligations to its customers. Thus, although organisations may not have thought about the data protection principles systematically, many **may already be complying** with a good number of the data protection principles without knowing it.

8. THE NIAC MODEL CODE

8.1 We should explain from the outset that the Model Code is intended to provide a broad and flexible framework based on the principles of the OECD Guidelines. The principles have thus been framed in general terms so that they may be applied by a wide range of organisations to the personal data they hold. The principles are designed to be flexible enough to take into account sectoral differences, variations in individual cases, and even the development of new technologies

8.2 However, it is not a case of "one size fits all", as we also recognise that data uses differ between sectors. While the principles in the Model Code are sacrosanct, organisations may "tailor" the wording of the Model Code to suit their own needs by developing codes of practice that explain how the principles will be implemented.[41] Thus, the Model Code also serves as a template upon which businesses or industries may base more refined, industry-specific, data protection codes.

Data Protection Instruments

8.3 The Subcommittee considered three sets of fair information principles, namely those contained in:

[41] Where "tailoring" ends and "dilution" begins can, of course, be a tricky question.

- The OECD Guidelines (1980);
- The EU Directive (1995); and
- The CSA Model Code (1996).

OECD Guidelines

8.4 Most of the world's data protection laws are based around sets of (variously named) information privacy principles which formally derive largely from two sources: the OECD Guidelines (1980) and the Council of Europe *Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data*[42].[43]

8.5 The OECD Guidelines are still in force. They have been a useful template and they have elicited certain commitments from major companies in the United States and Canada to adhere to information privacy principles. They continue to carry considerable force within the debates over the future of global e-commerce. However, the OECD Guidelines have been surpassed to some extent by the EU Directive, passed in 1995 to harmonise European data protection laws.

EU Directive

8.6 However, these early international data protection instruments were merely proposals that individual nations could take or leave at their choosing.[44] The need for a binding frame that would force all member states to adopt data protection laws was thus one of the major factors leading to the development of the EU Directive in 1995.

8.7 Four little words in this Directive mean that organisations outside Europe will have to take far more seriously their data protection commitments.[45] At this time, the Europeans are gradually clarifying how this provision is going to be enforced. Notwithstanding, the Legal Subcommittee took guidance from the EU Directive in formulating the Model Code. This is evident from the minutes of proceedings as well as the rest of this Report.

[42] (Convention No.108) in force since 1985.

[43] For the history behind the evolution of data protection in Europe, see the Conference Report, "*Data Protection in the Global Society*" (1996), *ibid* at fn 13.

[44] E.g. the Convention opened for signature in 1981, but many states either choose not to sign as in the case of Italy and Greece, or were not able to do so because they had no data protection provisions: "*Data Protection in the Global Society*", *ibid*.

[45] Article 25. Personal data may not be transferred outside European Member States unless the receiving jurisdiction can assure an "adequate level of protection".

CSA Code

8.8 The CSA Code is based on the OECD Guidelines. Canada was the first country in the world to establish a voluntary, national standard for the protection of personal information. The CSA Code is the result of a collaborative effort by representatives from all key groups concerned with privacy in Canada. The 45-member committee that developed the Code included representatives from such diverse sectors as the financial services, telecommunications, cable television and direct marketing industries; federal and provincial governments; consumer advocates; organised labour; and experts in security and information technology.

8.9 At first glance, the CSA Code might just seem a Canadian version of the OECD Guidelines -- a rearrangement and translation of the key principles into the Canadian context. Its real significance, however, is that it represents a consensus brokered among the major stakeholders.

8.10 A comparison of the CSA Code with those of other jurisdictions also reveals that the CSA Code is fairly representative of the typical data protection principles articulated by major jurisdictions[46]. The CSA Code has also recently become the framework for federal data protection legislation in Canada applicable to the private sector[47].

8.11 We think therefore that the CSA Code is an appropriate starting point for the consideration and development of a private sector code for Singapore. The 10 information privacy principles making up the CSA Code have been rigorously scrutinised by the Legal Subcommittee for their concordance with the Singapore business and regulatory environment and have been modified accordingly.

Data Protection Principles

8.12 The Model Code is organised around 11 data protection principles, roughly differentiated according to the various stages of data processing. With the exception of Principle 11 (which is optional), organisations must adopt all the data protection principles in their entirety – no “cherry-picking” in other words.

8.13 Comments and Guidelines on each of the 11 Data Protection Principles are detailed in the Table at *Annex 4*. However, the Legal Subcommittee hastens to highlight the caution of the OECD that:

[46] E.g. UK, New Zealand, Australia, Hong Kong.

[47] The *Personal Information Protection and Electronic Documents Act 2000*, effective 1 Jan 2001.

> *"The distinction between different activities and stages involved in the processing of data which are assumed in the principles, are somewhat artificial and it is essential that the principles are treated together and studied as a whole."*

Definition of Personal Data

8.14 The Model Code regulates the processing of all "personal data". This is defined as:

> *"data, whether true or not, in an electronic form, which relate to a living individual who can be identified –*
>
> *(a) from those data, or*
> *(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller."*

8.15 This definition is adapted from UK. In arriving at this definition, no less than nine different definitions of personal data / personal information were considered (see comparative table at *Annex 5*). The CSA Code's definition closely followed the early, OECD formulation drawn up in 1980. The EU Directive, in 1995, built on the OECD's definition by further defining "identifiable person". However, neither Canada (i.e. in the CSA Code, Privacy Act and PIPEDA) nor New Zealand has adopted this new development. In these jurisdictions, the meaning of "identifiable person" is left open. On the other hand, in UK, the criteria for linking identity to the data is clearly spelt out. Hong Kong and Australian legislation take after the UK (with minor variations).

"Whether true or not": Incorrect Data

8.16 Data may be false and judgements may be erroneous. Incorrect data can arise through inadvertent computer error, technical failure or intentional misuse. Such data should nonetheless fall within the data protection regime for the reason that incorrect data might influence decisions to the detriment of data subjects.[48]

[48] See our views above (at fn 43) about procedural fairness and natural justice as one of the goals of data protection.

8.17 Data protection extends beyond the protection of privacy[49] and does not recognise the same distinctions as the common law, which restricts a remedy for defamation to false statements injurious to reputation.[50]

"In an electronic form"

8.18 The focus of a data protection regime is on recorded data.[51] This contrasts with the common law duty of confidence, which focuses on any information disclosed in circumstances imposing the obligation, whether orally or recorded.[52] Data protection regimes regulate the disclosure of recorded data, although the disclosure itself may be in any form, including orally.

8.19 Non-automated records range from the systematic to the shambolic. The extent to which they are kept in an organised manner is generally related to the degree of risk posed of disclosure to third parties. Data relating to a data subject buried in an amorphous file and effectively irretrievable as a result would be less likely to be used or transmitted by the record-keeper. This focus on data that occasion specific risks to the data subject is reflected in the OECD Guidelines[53].

8.20 The EU Directive applies to personal data processed by automatic means (e.g. a computer database of customers) and to personal data that are part of or intended to be part of a non-automated "filing system" in which they are accessible according to specific criteria (e.g. traditional paper files, such as a card file with details of clients sorted in alphabetical order of the names): Article 3(1).

8.21 The Legal Subcommittee felt, however, that the Model Code should not at this stage apply to manual data, even if such data form part of a filing system, as the Subcommittee was unable to assess the impact of the operation of the Model Code to manual records. The Subcommittee felt that it would be difficult for manual filing systems to comply with some of the principles (in particular, access

[49] Which is generally thought to relate to protection from the disclosure of accurate information about a person.

[50] It is a complete defence that the statement is true.

[51] The principles recognise that the personal data regulated is often recorded with some degree of permanence - they refer to the collection of data, the provision of security safeguards, appointment of data controllers, rights of access and correction.

[52] In *Stephens v Avery* [1988] 2 All ER 545, it was held that the duty attached to the disclosure of information orally imparted in confidence. The disclosure was not of recorded data.

[53] The explanatory Memorandum comments that:

> *"The Guidelines therefore apply to personal data in general or, more precisely, to personal data which, because of the manner in which they are processed, or because of their nature or context, pose a danger to privacy and individual liberties."*

and accuracy). At a later stage, though, the scope of the Model Code could be extended to include manually-recorded personal data.[54]

8.22 A concern may be raised that this approach presents an incentive to businesses to abstain from automating their information systems in order to circumvent the principles in the Model Code. However, the Legal Subcommittee thinks that this does not pose any real threat in view of the benefits and rewards of being on the information highway.

"Which relate to a living individual"

8.23 This aspect of the definition could potentially be construed very widely. It will be a question of fact in each particular case whether or not data relate to a particular individual. One element to be taken into account is whether a data controller can form a connection between the data and the individual.

8.24 Data do not have to relate solely to one individual. The same set of data may relate to two or more people and still be personal data about each of them. For example, joint tenants of a property or holders of a joint bank account, or individuals who use the same telephone or email address.

8.25 Data may relate to an individual in a business capacity and not just to their private life. For example, the earnings of a sole proprietorship may amount to personal data of the individual sole proprietor. Similarly, data about an individual in a partnership may amount to personal data if it relates to a specific partner.

8.26 Thus, although the Code refers to individuals and not other legal entities such as associations or corporations,[55] there may be situations where data about an association or corporation or other legal entity can fairly be said to "relate to" a specific individual hence personal data. Data solely about the legal entity will however not be personal data.

[54] It has been said that often the most sensitive information continues to be held on manual files. (This was recognised in UK: see page 11, Hong Kong Law Reform Commission Report on "*Reform of the Law Relating to the Protection of Personal Data*", Aug 1994. More fundamentally, the practical distinction between computerised and manual records is breaking down with the development of optical scanners and the cross-referencing or tagging of one medium to the other.

[55] See discussion below under "Data Subjects"

"Who can be identified from…."

8.27 The individual must be capable of being *identified*. This might occur from the data itself[56], from data already in the possession of the data controller, or from data that is likely to come into the possession of, the data controller. Regarding the latter, it will be for the data controller to satisfy himself whether it is likely that such data will come into his possession to render data personal data. This will depend largely on the nature of the processing undertaken by the data controller.

> **Example:**
>
> CCTV footage may produce an image which is not of a distinguishable individual, but if the actual identity of that individual may become apparent from other information likely to come into the possession of the data controller (eg. if the image can be matched to a photograph, a physical description, or a physical person), then this is personal data.

8.28 A controversial issue relates to the profiling of a particular web user built up over a period of time (perhaps through the use of tracking technology or cookies) with no intention of linking it to a name and address or even an email address. There may not be any ability to locate that user in the *physical world*. One view (which the Legal Subcommittee does not necessarily agree with) is that in the context of the online world, data which uniquely locates an individual in *that* world, by distinguishing him from others, "identifies" him and is personal data.[57]

8.29 Finally, it should be noted that an individual may be "identified" without his name and address necessarily being known or revealed.

Non-sensitive Data

8.30 The Legal Subcommittee considered whether a data protection regime should only regulate data relating to an individual which it would be reasonable to expect him to regard as intimate or sensitive and therefore to want to withhold or at least to restrict their collection, use or circulation. It has been noted that:

[56] e.g. in the context of the Internet, many email addresses are personal data where the email address itself clearly identifies a particular individual.

[57] "*Legal Guidance: Data Protection Act 1998*", issued by the UK Information Commissioner. The Commissioner cautioned however that the thinking of her Office is still evolving, and that their advice in the Guidance may develop in certain areas in the light of case-law, etc.

> *"…if a loss of 'privacy' occurs whenever* any *information about an individual becomes known (the secrecy component) the concept loses its intuitive meaning."*[58]

8.31 This raises fundamental questions regarding the objectives of a data protection regime. Unfortunately, although the general inspiration for the development of data protection laws is apparent, the goals are rarely spelt out in satisfactory detail.[59] But as data protection regimes give effect to the data protection principles, their aims can be discerned from an examination of these principles. The combined effect of the principles can be described as ensuring that the right data are disclosed to the right person for the right purpose. The principles are not an end in themselves but are, it is suggested, about ensuring that *decisions* made on the basis of information affecting data subjects are fairly made, in a procedural sense.[60]

8.32 A feature of modern society is the propensity to accumulate data. The accumulation of seemingly trivial or non-sensitive data can result in the compilation of revealing profiles. Individual purchases may tell little about a person, but a comprehensive record over a period of time will describe the consumer's lifestyle.

8.33 For this reason we recommend that the data protection regime should be concerned with "personal data" in the sense of any representation of data relating to an identifiable individual and should not be restricted only to sensitive or intimate data.[61]

The Distinction between Information and Data

8.34 While "information" and "data" are used interchangeably in most literature, it appears that "data" has a wider meaning than "information". Professor Raymond Wacks states:[62]

[58] Raymond Wacks, *Personal Information: Privacy and the Law* (Oxford, Clarendon Press, 1989), page 16

[59] David Flaherty, *Protecting Privacy in Surveillance Societies* (University of North Carolina Press, 1989), page 30

[60] Akin to the common law rules of procedural fairness, or rules of natural justice, which has been summed up as providing that "persons must be afforded a fair and unbiased hearing before decisions are taken which affect them".

[61] This is consistent with the approach invariably adopted by the EU and in all other jurisdictions.

[62] Raymond Wacks, *Personal Information: Privacy and the Law* (Oxford, Clarendon Press, 1989), page 25

> *"'Data' become 'information' only when they are communicated, received and understood. 'Data' are therefore potential 'information'. Thus when the data assume the form of the printed word, they are immediately transformed into information by the reader. Where, however, data consists in acts or signs which require any meaning, they remain in this state of pre-information until they are actually understood by another."*[63]

8.35 A similar view was enunciated by Roger Clark:[64]

> *"The information systems discipline uses 'data' as a quite general term for any measurement of any real-world phenomenon. 'Information' is data which is pertinent to a particular decision, and hence data becomes information only in particular contexts. Such a distinction goes to the very heart of the important concept of 'relevance'. Most data protection regulation should therefore be concerned with 'data', although it may be appropriate to phrase some requirements in terms of 'information', in particular those matters relating to use and disclosure;*

8.36 The Legal Subcommittee accepts the reasoning of these distinguished authors and recommends the regulation of "personal data" instead of "personal information". This is the approach taken in the UK and Hong Kong legislation.[65]

Factual and Judgmental Data

8.37 Information about a person may be strictly factual and objective, such as a date of birth. Often, however, it may include an evaluative aspect, e.g. an opinion or judgement. To say that a person drinks a bottle of brandy daily is an assertion of fact, but one inviting the judgement that the person is an alcoholic.

8.38 The distinction is often a matter of form and difficult to draw. However, "judgmental" data will often be more influential than the factual basis they purport to convey. Accordingly, we recommend that personal data encompassing both

[63] By definition, encrypted data do not constitute "information".

[64] Roger Clark, "*The OECD Data Protection Guidelines: A Template for Evaluating Information Privacy Law and Proposals for Information Privacy Law*". The article is available online at http://www.anu.edu.au/people/Roger.Clarke/DV/PaperOECD.html

[65] cf. Canadian, Australian and New Zealand legislation which regulate information. The EU and OECD Models purportedly regulate data, however as "personal data" is defined as "information relating to an identified or identifiable….. person", these models in fact regulate information.

factual and judgmental data be regulated. This is the approach generally adopted in existing data protection laws.[66]

Data Subjects

8.39 The Model Code refers to the person to whom data are linked as the "data subject". We recommend that the data subject must be a *living* individual, as it would be too complex to extend regulation to the estates of deceased persons. This is the approach taken under the UK Data Protection Act 1998[67].

8.40 The Legal Subcommittee also considered whether data protection should apply not only to natural persons, but also to groups or classes of natural persons such as associations, and to legal persons such as companies and trusts.

8.41 The OECD had considered this issue and decided in favour of natural persons only, on the basis that " *... individual integrity and privacy are in many respects particular and should not be treated in the same way as the integrity of a group of persons, or corporate security and confidentiality*".

8.42 The Legal Subcommittee accepts the reasoning of the OECD and recommends that the Code should apply only to data about "individuals". This excludes corporations or associations who, though they are "legal persons", are not individuals.

Territorial scope

8.43 In respect of a data user, the Model Code applies to any personal data *processed in Singapore*, regardless of whether the data controller is within Singapore.

8.44 Equally, data processing outside Singapore that is *controlled from within Singapore* is also subject to the provisions of the Code[68].

8.45 Certain foreign data protection regimes surveyed restrict the scope of protection depending on the *status of the data subject*, e.g.:

[66] Law Reform Commission of Hong Kong's *Report on Reform of the Law Relating to the Protection of Personal Data (Topic 27)* at page 82.

[67] Definition of "personal data" in s.1

[68] As in UK. There is also the practical consideration that if data is not processed or controlled within Singapore, effective enforcement by any local oversight agency is precluded.

- use of the term "citizen" (rather than "person") – this disqualifies all non-citizens, a not insignificant proportion of the population of many countries especially Singapore[69];

- restriction to people "resident" in the country – this disqualifies not only tourists, but also people (even citizens) whose residence is too short-term or sporadic;

- restriction to persons "in the country" – this disqualifies not only aliens but also citizens during their absence from the country.

8.46 The Legal Subcommittee recommends that the Code should apply in an unqualified manner in favour of all data subjects dealing with the data user. This is also consistent with the Article 25 of the EU Directive, which seeks to protect the personal data of EU subjects.

Onward Transfers of Personal Data

8.47 Based on the above, if data are transferred out of the organisation, but control is retained within the organisation (e.g. transfer to a data bureau solely for processing and return to the organisation for use), the data should remain subject to the general application of the Code.

8.48 Onward transfers of data either for *public purposes* or for purposes which involve the *consent* of the data subject should not be subject to additional controls, even when the transfer of data is accompanied by a *loss of control* over the data.

8.49 Outside of these categories, however, onward transfers should be regulated, otherwise the integrity of the data may be compromised. Principle 11 prevents the organisation from transferring data to any recipient outside Singapore, unless an adequate level of protection is assured. The principle is based on the restrictions on international transfers of personal data set out in Article 25 of the EU Directive.

8.50 The exchange of data is primarily an electronic processing phenomenon but non-automated exchanges such as posted mail or tape recordings also occur. The Model Code regulates only electronic data; however, insofar as electronic data are concerned, the mode of transfer is irrelevant.[70]

[69] One out of four people living in Singapore is a foreigner, according to the Department of Statistics.
[70] Other data protection laws encompassing manually processed data (e.g. France, Germany, and the Netherlands) envisage a similarly broad application to the transfer of data.

Importation of Personal Data

8.51 Upon importation of personal data into Singapore, the data protection principles apply. The data subject is entitled to challenge the data whether or not he resides in Singapore. Access and correction rights are not restricted to Singapore residents.

Existing Records/Transition Period

8.52 The Legal Subcommittee recognised that the adoption of the Model Code involves a major exercise by organisations in putting their data in order. It also requires the co-operation of data subjects in updating their data. Thus, the Subcommittee felt that it would be unfair to subject the organisation immediately to the full force of the Model Code.

8.53 On the other hand, the Subcommittee rejected the alternative position: that the Model Code should apply only to personal data generated after the Model Code is adopted by the organisation. This option was rejected on practical grounds and on principle. On practical grounds, it would be operationally difficult, if not impossible, to distinguish between personal data held before and after a particular date. On principle, the Subcommittee felt that it was unfair to permanently deny access and correction rights to existing personal data or to sanction the continued use or retention of personal data not collected or maintained in accordance with the principles.

8.54 A good compromise between the two alternatives is for the Model Code to be implemented in phases, and for the provision of transitional provisions.

8.55 We accordingly recommend that upon adoption of the Model Code, the Code apply to all personal data already in existence. However, the following principles shall only apply after a transition period of one year:

(i) **Principle 6 (Accuracy)** – i.e. there would be no breach of this principle during the transition period;

(ii) **Principle 9 (Access)** – i.e. the data user would not be required to provide a full copy of all data held at the time of the request, but would be entitled to first clean up the data by updating and removing irrelevant or dubious data. The data user would then be obliged to provide the data subject with a copy of all the remaining data.

Exemptions

8.56 Having surveyed the data protection regimes in various jurisdictions, we observe that certain types of data processing are exempted from the application from some or all of the data protection rules. Depending on the jurisdiction, they may include any or all of the following:

1. General Exemptions:

(a) Processing by any individual in respect of personal information for **personal** or **domestic use** only;

(b) Processing by any organisation in respect of personal information for **journalistic**, **artistic** or **literary** purposes only;

(c) Processing of **employment data**;

(d) Any processing operations which are necessary to safeguard:

(i) national security;
(ii) defence;
(iii) public security;
(iv) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
(v) an important economic or financial interest of Singapore;
(vi) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (iii), (iv) and (v);
(vii) the protection of the data subject or of the rights and freedoms of others; and

(e) Processing of personal data for **scientific research** or for the sole purpose of creating **statistics**.

2. Specific Exemptions:

2.1 Collection by organisation without knowledge or consent of individual

(a) Collection is **clearly in the interests of the individual** and consent cannot be obtained in a timely way;

(b) Collection with the knowledge or consent of the individual would **compromise the availability or the accuracy of the information** where such collection pertains to an investigation of a breach of an agreement or the law;

(c) Collection is solely for **journalistic**, **artistic** or **literary purposes**;

(d) Information is **publicly available**.

2.2 Use by organisation without knowledge or consent of individual & Use by organisation of information for purposes other than those for which it was collected

(a) Used in the **investigation of an illegal act** that has been, is being or is about to be committed;

(b) Used in an **emergency that threatens the life, health or security** of an individual;

(c) Used for **statistical, or scholarly study or research that cannot be achieved without use of the information, if**:

- information is used in a manner that ensures its confidentiality;
- it is impractical to obtain consent; and
- organisation informs the Commissioner of the use ;

(d) Information is **publicly available**;

(e) Information was collected under **paragraphs 2(a) or 2(b)**.

2.3 Disclosure by organisation without knowledge or consent of individual

(a) Made to **solicitor** who is representing the organisation;

(b) For **collecting a debt** owed by the individual;

(c) To **comply with a subpoena** or warrant with jurisdiction to compel the production of information;

(d) To a **government institution that has made a lawful request** for information and has indicated that:
- information relates to **national security**, the **defence** of the nation or the conduct of **international affairs**;
- disclosure is for the purpose of **enforcing any law** of the nation or a foreign jurisdiction;
- disclosure is for the purpose of **administering any law** of the nation;

(e) Made on the **initiative of the organisation to an investigative body** or a government institution:
- information relates to a **breach of agreement or an illegal act** that has been, is being or is about to be committed;
- information relates to **national security**, the defence of the nation or the conduct of international affairs;

(f) Made to a person who needs the information because of an **emergency** that threatens the life, health or security of an individual and, if the individual whom the information about is alive, the organisation informs that individual in writing without delay of the disclosure;

(g) For **statistical or scholarly study or research** that cannot be achieved without disclosing the information, and:
- it is impracticable to obtain consent; and
- the organisation informs the Commissioner of the disclosure before it is disclosed;

(h) To an institution whose purpose is the conservation of records of **historic or archival importance** and disclosure is for such purpose;

(i) Made after the earlier of:
- 100 years after the record was created; and
- 20 years after the death of the individual whom the information is about;

(j) Information is **publicly available**;

(k) Made by an investigative body for purposes related to the investigation of a **breach of an agreement** or contravention of the law;

(l) **Required by law**.

2.4 When organisation not required to/prohibited from giving access to personal information

(a) When access is prohibited:

(i) If doing so would likely **reveal personal information about a third party** unless:
- the information about the third party is severable
- third party consents to the access
- individual's life, health or security is threatened

(ii) **Investigative body/government institution objects** to the organisation's complying with an individual's request to be informed of disclosures made under paragraph 4(c), (d) and (e) and compliance could reasonably be expected to be injurious to:
- national security, the defence of the nation or the conduct of international affairs
- the enforcement of any law of the nation or law of a foreign jurisdiction

(b) When access may be refused:

(i) Information is protected by **solicitor-client privilege**;
(ii) To do so would reveal **confidential commercial information**;
(iii) To do so would **threaten the life** or security of another individual;
(iv) The information was collected under **paragraph 2(b)**

8.57 The CSA Code does not spell out any exemptions (whether general or specific) but leaves this open for the particular industry or organisation to decide. However, in the Singapore context, the Legal Subcommittee felt that the approach taken in legislation (which is to exhaustively set out all the permitted exemptions, general and specific) is preferred. We have accordingly incorporated an exhaustive list of such exemptions into the Model Code.

9. SUMMARY OF RECOMMENDATIONS

9.1 The main recommendations of the Legal Subcommittee are:

6.1.8 Effective protection of personal data is desirable in the Singapore private sector.

6.1.9 The data protection regime for the private sector should be founded on internationally recognised standards of data protection.

6.1.10 As an interim measure, voluntary data protection guidelines for the private sector (such as the Model Code) should be given official recognition and adherence invited on a voluntary basis. The exercise will have an educative and harmonising function and should facilitate the introduction of legislation, should Parliament decide in the future to legislate.

6.1.11 In the longer term, it remains to be seen whether a reliance on voluntary controls in the private sector would be completely effective or whether an appropriate degree of legislative intervention may be required. This would depend on the response of industry and consumers to the self-regulatory regime.

6.1.12 The data protection regime should be concerned with "personal data" in the sense of any representation of data, true or not, factual or judgmental, relating to a living individual whose identity is either apparent from the data, or can be reasonably ascertained. All data that are capable of being read intelligibly should be covered. The regime should not merely cover "sensitive" or "intimate" data. However, the level of protection will depend on the sensitivity of the data.

6.1.13 At this stage, the data protection regime should apply only to the processing of data wholly or partly by automated means. For practical reasons, the regime should not at this stage apply to processing of data otherwise than by automatic means, even if such data form part of a filing system or are intended to form part of a filing system. It would be difficult for manual filing systems to comply with some of the principles (e.g. access and accuracy). But if manual data are subsequently converted to electronic form, the data processor will, from that point onwards, be required to comply with the Model Code.

6.1.14 The data protection principles should immediately apply to data in existence upon adoption of the Model Code. However, the following principles will only apply after a transition period of one year:

(iii) **Principle 6 (Accuracy)** – i.e. there would be no breach of this principle during the transition period;

(iv) **Principle 9 (Access) –** i.e. the data user would not be required to provide a full copy of all data held at the time of the request, but would be entitled to first clean up the data by updating and removing irrelevant or dubious data. The data user would then be obliged to provide the data subject with a copy of all the remaining data.

6.1.12 The data protection regime should apply to any personal data *processed or controlled* in Singapore, regardless of whether the data controller is within Singapore.

6.1.13 The data protection regime should apply in favour of all data subjects, whether or not they are resident in Singapore. In particular, access and correction rights should not be restricted to Singapore residents.

6.1.14 The data protection regime should prevent organisations from transferring any data which would involve a loss of control over the data, to any recipient within or outside Singapore unless certain conditions are met.

6.1.15 Certain types of data, and certain types of data processing, may be exempted from the application from some or all of the data protection rules.

10. CONCLUSION

10.1 This report proposes the adoption of a comprehensive data protection regime for the private sector. The adoption of the standards in the Model Code is a significant step forward, whether this is done as part of a voluntary scheme, or in conjunction with legislation.

10.2 The first step, if action is to be taken on the issue of data protection, is to agree on the principles that a data protection regime should promote. This is the substance of the NIAC Model Code. The second step would be to decide on the best approach to ensure compliance with those principles, i.e. whether self-regulation; co-regulation, "light-touch" legislation, or "heavy" prescriptive legislation.

10.3 Insofar as the issue of costs is concerned, it is certainly true that implementation of the data protection principles requires changes to be made. There is the cost of revamping current systems[71]. There is also the cost of devoting human resources to co-ordinating and drawing up procedures for compliance with the Model Code. For organisations already involved in global e-commerce, costs of compliance would be kept to a minimum since the Model Code follows the common overseas model.

10.4 In any event, whatever the price tag involved, this must be viewed against the benefits. Successful implementation of the data protection principles sends a positive message to customers and employees. This is good for customer and employee relations. Implementation of the data protection principles is also an opportunity to get to grips with data collection, holding and processing systems that may no longer be fully under control. Improvements in these areas should bring operational efficiency and planning gains.

[71] For example, to include statements of the purpose of collecting personal information in customer forms and to ensure the erasure of personal information when the original purposes of collection have been fulfilled.

10.5 At a higher level, comfort should be taken from the fact that the implementation of an adequate data protection regime means that Singapore comes up to the international standard that other places with such laws wish to see. As a result, there should be no reason for interference by those other places in the free flow of personal data to Singapore on which trade, particularly in the service industries, crucially depends.

ANNEX 1

Legal Subcommittee Members 2001

Chairman:
Mr Charles Lim Aeng Cheng
Head, Law Reform and Revision Division
Attorney-General's Chambers
1 Coleman Street, #10-00,
Singapore 179803

Secretary:
Mr Vincent Kor
Senior Legal Manager
Policy & Planning Division
Singapore Broadcasting Authority
140 Hill Street
MITA Building, #04 - 01
Singapore 179369

Mr Edison Foo
General Counsel, Asia Pacific
Ariba Singapore Pte Ltd
UOB Plaza 1, 34th Floor
80 Raffles Place
Singapore 048624

Dr Ang Peng Hwa
Vice-Dean
School of Communication and Information
Nanyang Technological University
Nanyang Avenue
Singapore 639798

Mr Lawrence Tan
Manager
Development Policy
Infocomm Development Authority of Singapore
8 Temasek Boulevard
#14-00 Suntec Tower 3
Singapore 038988

Assoc Prof Yeo Tiong Min
Associate Professor
13 Law Link
Faculty of Law
National University of Singapore
Singapore 117590

Mr Gilbert Leong
IP & E-commerce Counsel,
GE Medical Systems, Asia
298 Tiong Bahru Road, #15-01/06
Central Plaza, Singapore 168730

Mr Lim Chin Tiak
Asst Director, Operations
Criminal Investigation Department
Singapore Police Force
Ministry of Home Affairs
90 Eu Tong Sen Street
Singapore 059811

Mr Daniel Seng Kiat Boon
Research Director
Singapore Academy of Law
3 St Andrew’s Road
#03-00 City Hall
Singapore 178958

Mr Tan Ken Hwee
State Counsel
Attorney-General’s Chambers
International Affairs Division
1 Coleman Street, #10-00,
Singapore 179803

Mr Jim Lim Kheng Huat
M/s Shook Lin & Bok
1 Robinson Road
#18-00 AIA Tower
Singapore 048542

Mr Lionel Tan I-Kwok
Partner
M/s Rajah & Tann
4 Battery Road #26-01
Bank of China Building
Singapore 049908

Ms Wendy Yap Peng Hoon
State Counsel
Attorney-General’s Chambers
Law Reform and Revision Division
1 Coleman Street, #05-04,
Singapore 179803

Ms Aileen Koh
Legal Counsel / Manager
Accenture, Legal & Commercial Group
152 Beach Road
#19-00 Gateway East
Singapore 189721

Mr Lim Seng Siew
Chief Executive Officer
The Portal WWLegal.com Pte Ltd
9B Circular Road
Singapore 049365

Ms Lau Joon-Nie
Deputy Chief Editor, E-News
MediaCorp News Pte Ltd
Caldecott Broadcast Centre
Andrew Road
Singapore 299939

Mr Christopher Tang
Partner
M/s Allen & Gledhill
36 Robinson Road
#18-01 City House
Singapore 068877

SINGAPORE ACTS PROVIDING STATUTORY SECRECY AND DISCLOSURE PROVISIONS (as at 1999)

1. ACCOUNTANTS ACT
2. ADMINISTRATION OF MUSLIM LAW ACT
3. ADVANCE MEDICAL DIRECTIVE ACT
4. AIR NAVIGATION ACT
5. ARCHITECTS ACT
6. AUDIT ACT
7. BANKING ACT
8. BANKRUPTCY ACT
9. BETTING ACT
10. CENSUS ACT
11. CENTRAL PROVIDENT FUND ACT
12. CHARITIES ACT
13. CHILD CARE CENTRES ACT
14. CHIT FUNDS ACT
15. CINEMATOGRAPH FILM HIRE DUTY ACT
16. CIVIL AVIATION AUTHORITY OF SINGAPORE ACT
17. CIVIL DEFENCE ACT
18. COMMERCIAL AND INDUSTRIAL SECURITY CORPORATION ACT
19. COMMODITY FUTURES ACT
20. COMMON GAMING HOUSES ACT
21. COMMUNITY MEDIATION CENTRES ACT
22. COMPANIES ACT
23. COMPUTER MISUSE ACT
24. CONSTITUTION OF THE REPUBLIC OF SINGAPORE
25. CONSTRUCTION INDUSTRY DEVELOPMENT BOARD ACT
26. CONSUMER PROTECTION (TRADE DESCRIPTIONS AND SAFETY REQUIREMENTS) ACT
27. CONTROL OF ESSENTIAL SUPPLIES ACT
28. CONTROL OF MANUFACTURE ACT
29. CONTROLLED PREMISES (SPECIAL PROVISIONS) ACT
30. CO-OPERATIVE SOCIETIES ACT
31. COPYRIGHT ACT
32. COUNTERVAILING AND ANTI-DUMPING DUTIES ACT
33. CRIMINAL LAW (TEMPORARY PROVISIONS) ACT
34. CRIMINAL PROCEDURE CODE
35. CURRENCY ACT
36. CUSTOMS ACT
37. DRUG TRAFFICKING (CONFISCATION OF BENEFITS) ACT

38. ECONOMIC EXPANSION INCENTIVES (RELIEF FROM INCOME TAX) ACT
39. EDUCATION ACT
40. ELECTRONIC TRANSACTIONS ACT
41. EMERGENCY (ESSENTIAL POWERS) ACT
42. EMPLOYMENT ACT
43. ENLISTMENT ACT
44. ENTERTAINMENTS DUTY ACT
45. ENVIRONMENTAL PUBLIC HEALTH ACT
46. ESTATE DUTY ACT
47. EVIDENCE ACT
48. EXCHANGE CONTROL ACT
49. FACTORIES ACT
50. FINANCE COMPANIES ACT
51. FINANCIAL PROCEDURE ACT
52. FIRE SAFETY ACT
53. FUTURES TRADING ACT
54. GENEVA CONVENTIONS ACT
55. GOODS AND SERVICES TAX ACT
56. GOVERNMENT PROCEEDINGS ACT
57. HINDU ENDOWMENTS ACT
58. HOMES FOR THE AGED ACT
59. HOUSE TO HOUSE AND STREET COLLECTIONS ACT
60. HOUSING AND DEVELOPMENT ACT
61. HOUSING DEVELOPERS (CONTROL AND LICENSING) ACT
62. HUMAN ORGAN TRANSPLANT ACT
63. IMMIGRATION ACT
64. INCOME TAX ACT
65. INDUSTRIAL RELATIONS ACT
66. INFECTIOUS DISEASES ACT
67. INLAND REVENUE AUTHORITY OF SINGAPORE ACT
68. INSTITUTE OF TECHNICAL EDUCATION ACT
69. INSURANCE ACT
70. INTERNAL SECURITY ACT
71. INTERNATIONAL ARBITRATION ACT
72. INTOXICATING SUBSTANCES ACT
73. KIDNAPPING ACT
74. LAND ACQUISITION ACT
75. LAND SURVEYORS ACT
76. LAND TITLES (STRATA) ACT
77. LAND TITLES ACT
78. LAND TRANSPORT AUTHORITY OF SINGAPORE ACT
79. LEGAL PROFESSION ACT
80. MAINTENANCE OF RELIGIOUS HARMONY ACT

81. MARINE INSURANCE ACT
82. MARITIME AND PORT AUTHORITY OF SINGAPORE ACT
83. MEDICAL REGISTRATION ACT
84. MEDICINES (ADVERTISEMENT AND SALE) ACT
85. MEDICINES ACT
86. MERCHANT SHIPPING ACT
87. MISUSE OF DRUGS ACT
88. MONETARY AUTHORITY OF SINGAPORE ACT
89. MONEYLENDERS ACT
90. MOTOR VEHICLES (THIRD PARTY RISKS AND COMPENSATION) ACT
91. MUTUAL BENEFIT ORGANISATIONS ACT
92. NATIONAL ARTS COUNCIL ACT
93. NATIONAL COMPUTER BOARD ACT
94. NATIONAL COUNCIL OF SOCIAL SERVICE ACT
95. NATIONAL HERITAGE BOARD ACT
96. NATIONAL LIBRARY BOARD ACT
97. NATIONAL PARKS ACT
98. NATIONAL SCIENCE AND TECHNOLOGY BOARD ACT
99. NATIONAL SERVICEMEN (EMPLOYMENT) ACT
100. NEWSPAPER AND PRINTING PRESSES ACT
101. NGEE ANN POLYTECHNIC ACT
102. NURSES AND MIDWIVES ACT
103. OFFICIAL SECRETS ACT
104. PARLIAMENT (PRIVILEGES, IMMUNITIES AND POWERS) ACT
105. PARLIAMENTARY ELECTIONS ACT
106. PATENTS ACT
107. PAYROLL TAX ACT
108. PENAL CODE
109. PEOPLE’S ASSOCIATION ACT
110. POLICE FORCE ACT
111. PORT OF SINGAPORE AUTHORITY ACT
112. POST OFFICE SAVINGS BANK OF SINGAPORE ACT
113. PRESIDENTIAL ELECTIONS ACT
114. PREVENTION OF CORRUPTION ACT
115. PRISONS ACT
116. PRIVATE HOSPITALS AND MEDICAL CLINICS ACT
117. PRIVATE INVESTIGATION AND SECURITY AGENCIES ACT
118. PROFESSIONAL ENGINEERS ACT
119. PROPERTY TAX ACT
120. PUBLIC SERVICE COMMISSION ACT
121. PUBLIC TRUSTEE ACT
122. PUBLIC UTILITIES ACT
123. RADIATION PROTECTION ACT

124. REGISTRATION OF DEEDS ACT
125. REGULATION OF IMPORTS AND EXPORTS ACT
126. ROAD TRAFFIC ACT
127. SALE OF DRUGS ACT
128. SALE OF FOOD ACT
129. SALE OF GOODS (UNITED NATIONS CONVENTION) ACT
130. SCIENCE CENTRE ACT
131. SECURITIES INDUSTRY ACT
132. SENTOSA DEVELOPMENT CORPORATION ACT
133. SINGAPORE ARMED FORCES ACT
134. SINGAPORE BROADCASTING AUTHORITY ACT
135. SINGAPORE CORPORATION OF REHABILITATIVE ENTERPRISES ACT
136. SINGAPORE POLYTECHNIC ACT
137. SINGAPORE PRODUCTIVITY AND STANDARDS BOARD ACT
138. SINGAPORE SPORTS COUNCIL ACT
139. SINGAPORE TOTALISATOR BOARD ACT
140. SKILLS DEVELOPMENT LEVY ACT
141. STATE IMMUNITY ACT
142. STATES OF MALAYA CUSTOMS DUTIES COLLECTION ACT
143. STATISTICS ACT
144. STATUTORY BODIES AND GOVERNMENT COMPANIES (PROTECTION OF SECRECY) ACT
145. STREET WORKS ACT
146. SUPREME COURT OF JUDICATURE ACT
147. TELECOMMUNICATIONS ACT
148. TERMINATION OF PREGNANCY ACT
149. TIN AND TIN-ORE (DISCLOSURE OF SMELTERS' STOCKS) ACT
150. TITLES ACT
151. TOWN COUNCILS ACT
152. TRADE DEVELOPMENT BOARD ACT
153. TRADE MARKS ACT
154. TRADE UNIONS ACT
155. TRAVEL AGENTS ACT
156. URBAN REDEVELOPMENT AUTHORITY ACT
157. VIGILANTE CORPS ACT
158. VOCATIONAL AND INDUSTRIAL TRAINING BOARD ACT
159. VOLUNTARY STERILIZATION ACT
160. WATER POLLUTION CONTROL AND DRAINAGE ACT
161. WEIGHTS AND MEASURES ACT

Enforcement and Compliance Options for a Personal Data Protection Regime for the Private Sector in Singapore

Option	Pros	Cons
Comprehensive legislation (directive-based; covers all industries, private and public sectors) <u>Variant:</u> Separate comprehensive laws for private sector and public sector respectively	(1) Guaranteed satisfaction of EU Directive and other countries' data protection laws possible, thus avoiding restrictions on data transfers. (2) Consistent with current global trends, thus allowing a "seamless" transfer of data internationally. Consistency with international statutory regimes also minimises compliance costs for organisations. (3) Allows seamless transfer of data between different sectors within Singapore.	(1) Over-regulation may be onerous on businesses, and is inconsistent with Singapore's policy of minimising regulatory constraints and compliance costs. (2) Cost of setting up a national supervisory authority and recurring operational costs
Sectoral legislation (directive-based; addresses only "high risk" industry sectors or where need to protect consumer confidence is particularly high)	(1) Minimal regulation by government (compared to comprehensive legislation) as only "high-risk" sectors are legislated. (2) Provides scope for flexibility, allowing rules to be varied or stated in a different manner according to legitimate needs of each sector. Remedies can be provided in the context of own environment. (3) Clarity and specific content can be added to rules. Complex exceptions designed for other sectors can be omitted.	As in (1) and (2) above + (3) This approach does not reflect the growing convergence of many industries in each others' markets. Ignores reality that sectoral boundaries are becoming increasingly blurred and do not provide any impediment to the flow of data. (4) Piecemeal approach gives rise to 'boundary' issues where data is transferred to an unregulated sector or sector which is regulated by a different set of rules. Could give rise to an uneven playing field. (5) Complicated from data subjects' perspective, as similar types of data receive different treatment depending to sector in which they are located. (6) Unregulated sectors are still at risk of EU data restrictions

Option	Pros	Cons
Comprehensive Code of Practice (voluntary scheme; pure self-regulation) <u>Variants:</u> Standards-based/other audited schemes, eg. eTRUST	(1) Allows seamless transfer of data between different sectors within Singapore (2) One view is that a voluntary scheme avoids onerous costs in complying with a legislative regime (but see Moira Paterson's article, referred to in text of Report).	(1) Danger of imposition of restrictions on data transfers to Singapore by foreign countries because of lack of adequate compliance mechanisms. (2) Effective only to the extent that businesses choose to become a part of it. Does not adequately deal with less responsible businesses looking for short-term gains. This deters other businesses from opting into the scheme for fear of being placed at a cost disadvantage. (3) Does not have sufficient external, independent oversight and redress mechanisms to generate public confidence. (4) Very difficult to organise, requires one sector to take the initiative and "galvanise" other sectors.
Sectoral Codes of Practice (voluntary scheme; pure self-regulation)	As in (2) and (3) under Sectoral Legislation + (3) Easier to organise	As in (1), (2) and (3) above + piecemeal approach and "boundary" issues above + (6) Care needs to be taken to ensure that the consultation process is not unduly dominated by the large players and that any code that results is not unduly oppressive for smaller businesses.

Option	Pros	Cons
Co-Regulatory Schemes (self-regulation within a legislative framework)	When compared with pure, directive-based legislative schemes: (1) Encourages continuous and innovative self-improvement by giving business greater flexibility, within a clear framework of societal expectations and requirements, rather than stopping at compliance with a set performance or standard. Puts to good use the entrepreneurial dynamism and informational advantages of the business sector and promotes active involvement of the business community in the policy-making process. (2) Reduces dependency on limited government resources by making use of industry's knowledge and resources, thus reducing the expense of governments' having to collect the information, develop this into regulations, and then monitor the effects, often without an appropriate level of industrial and process experience. Compared with a pure self-regulatory schemes: (1) Government intervention is more likely to be effective in securing the collective action of sectoral organisations. (2) Governments is in a good position to promote international cooperation and harmonisation of self-regulatory schemes (3) can help forge global links between national schemes.	(1) Question remains whether "co-regulatory" instruments may be successfully introduced in countries that lack the tradition of the strong enforcement of data protection law. It has been said that partnership approaches are likely to be more effective when policies have matured beyond a level of 'basic regulation'.

	Example	**Comments**
	New Zealand Privacy Act 1993 – Privacy Commissioner may approve Codes which then replace legislative principles.	NZ – appears to have been “very successful in terms of maximising advantages while avoiding potential pitfalls”. Adoption of industry codes to date the exception rather than the rule. “No evidence of any widespread dissatisfaction by businesses or undue complication of legal framework.”
	Data Protection Act 1984 (Ireland) – as in NZ but codes must be approved by both the Data Protection Commissioner and Parliament.	Ireland – Advantage of ensuring continuing political oversight. But reduces the flexibility of the process.
	Netherlands Data Protection Act 1877 – codes have a lesser legal status. Registration of code has no legal force in the sense that breach of them is treated as breach of the Act, but it may have an evidentiary effect in assisting to establish liability under the Act.	Netherlands – emphasises the primacy of the data protection principles by ensuring that they cannot be diluted by the registration of codes. But open to criticism that it creates more uncertainty for businesses.
	Hong Kong Personal Data (Privacy) Ordinance 1995 – provides that a failure to observe any provision of an approved code does not of itself give rise to any legal liability but may have some evidentiary effect in establishing liability under the Act (similar to Netherlands model)	Hong Kong – HK Law Reform Commission took the view that the data protection principles were flexible enough to take account of “sectoral differences, the variation of individual cases and the development of new technologies”. It recommended against imposing legal liability on the ground that it would divert resources away from encouraging compliance with the principles.

	Example	Comments
	UK Data Protection Act 1984 – legislation makes provision for codes which do not have any legal status. UK Data Protection Registrar has a duty to encourage trade associations and data users to prepare and disseminate codes of practice for guidance in complying with the data protection principles.	UK – approach provides for little incentive to industries to develop codes. The lack of provision for oversight of codes may result in a situation where codes may be positively misleading and therefore counter-productive.
	Australian Privacy Amendment (Private Sector) Act 2000 – The National Privacy Principles set the base line standards for privacy protection. However, the Privacy Commissioner may approve legally binding codes, to be adopted and enforced by organisations or industries, in place of the NPPs (similar to NZ model).	Australia – a notable feature of the scheme is the seamless interface between the public and private sectors. But it is open to criticism by the private sector that the principles are both complex in their wording and specifically designed for the public sector. In addition the principles have been criticised as being outdated and inadequate to deal with the problems posed by modern technological developments.

ANNEX 4

National Internet Advisory Committee ("NIAC") Model Code	**Guidelines and Comments by the Legal Subcommittee of the NIAC**
Scope This Model Code describes the minimum requirements for the protection of personal information in the form of electronic data ("personal data"). Any applicable legislation must be considered in implementing these requirements. **1.2** Provided the minimum requirements are met, organisations may tailor this Model Code to meet their specific circumstances. For example, policies and practices may vary, depending upon whether the personal data relate to members, employees, customers, or other individuals. **1.3** The objective of this Model Code is to assist organisations in developing and implementing policies and practices to be used when managing personal data.	[Paragraphs 1 - 1.3 are adapted from the *Canadian Standards Association's Model Code for the Protection of Personal Information 1996* ('CSA Code').] Comments: ▪ Background to the CSA Code The CSA Code was drafted based on the *1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* ('OECD Guidelines'). Canada was the first country in the world to establish a voluntary, national standard for the protection of personal information. The CSA Code was the result of a collaborative effort by representatives from all key groups concerned with privacy in Canada. The 45-member committee that developed the CSA Code included representatives from such diverse sectors as the financial services, telecommunications, cable television and direct marketing industries, federal and provincial governments, consumer advocates, organised labour, and experts in security and information technology. The CSA Code is fairly representative of the typical data protection principles articulated by major jurisdictions and has recently become the framework for federal data protection legislation in Canada applicable to the private sector (*Personal Information Protection and Electronic Documents Act 2000*) (*'PIPEDA'*). ▪ General Guidelines on Model Code: The Model Code is intended to provide a broad and flexible framework based on the principles of the OECD Guidelines. The principles have been framed in general terms so that they may be applied across sectors by a wide range of organisations.

National Internet Advisory Committee ("NIAC") Model Code	Guidelines and Comments by the Legal Subcommittee of the NIAC
	However, it is also recognised that data users and uses may vary significantly between sectors. If this is the case, the Model Code may, as an alternative, be used as a template upon which businesses or industries may base more industry-specific data protection rules.
1.4 Where appropriate, the following data processing activities may be exempted: (a) Processing required by any **law** or by the **order of a court**; (b) Processing by any individual purely for that individual's **personal, family, or household affairs (including recreational purposes)**; (c) Processing of personal data purely for **journalistic**, **artistic** or **literary** purposes; (d) Processing of **employment data**; (e) Any processing operations which are necessary to safeguard: (viii) National security; (ix) Defence; (x) Public security; (xi) The prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (xii) An important economic or financial interest of Singapore; (xiii) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (iii), (iv) and (v); (xiv) the protection of the data subject or of the rights and freedoms of others; and (e) Processing of personal data for **research** or for the purpose of creating **statistics**, provided the results of the research or any resulting statistics are not made available in a form which identifies data subjects or any of them.	[Paragraphs 1.4 - 1.6 are not found in the CSA Code and have been inserted by the Legal Subcommittee.] Comments: ▪ Having surveyed the regimes in various jurisdictions, we observe that certain types of data processing are generally exempted. The exemptions adopted here are generally based on those in Canadian legislation in respect of the private sector (Personal Information Protection and Electronic Documents Act 2000), and the EU Directive (Articles 3 and 13). ▪ Employment data were excluded from the Model Code because of its burden on employers, affecting competitiveness. However, the Subcommittee noted that EU has criticised Australia for exempting employment data. The EU commented that such information is often very sensitive and should be protected. The Canadian PIPEDA exempts general employment information (name, title, business address and telephone number) from the definition of "personal information". Despite the Code's exemption of employment data, organisations may opt to restrict this exemption only to such processing activities necessary for the purposes of carrying out their obligations under the employment relationship.

National Internet Advisory Committee ("NIAC") Model Code	Guidelines and Comments by the Legal Subcommittee of the NIAC
1.5 The Model Code applies to the processing of personal data wholly or partly by automatic means.	Organisations are of course free to additionally subject their manual filing systems to the operation of the code, on a voluntary basis. Manual data subsequently converted into electronic form will be subject to the Model Code from that point onwards and the data processor will be required to comply with the Model Code. Comments: ▪ The CSA Code does not specify whether only data processed by automated means are covered under the Code, or if non-automated data are also included. ▪ The EU Directive (Article 3(1)) applies to personal data processed by automated means (e.g. a computer database of customers) and to personal data that are part of or intended to be part of a non-automated "filing system" in which they are accessible according to specific criteria (e.g. traditional paper files, such as a card file with details of clients sorted in alphabetic order of the names). ▪ The Subcommittee felt that the Model Code should not at this stage apply to manual data, even if such data form part of a filing system or are intended to form part of a filing system, as the Subcommittee was unable to assess the impact of the operation of the Model Code to manual records. The Subcommittee felt that it would be difficult for manual filing systems to comply with some of the principles (e.g. access and accuracy).

National Internet Advisory Committee ("NIAC") Model Code	Guidelines and Comments by the Legal Subcommittee of the NIAC
1.6 The Model Code applies to any personal data which are processed or controlled by the organisation, regardless of whether the data are transferred out of Singapore. The Model Code applies in favour of all data subjects, whether resident in Singapore or not, whose data are or have been processed by the organisation.	Comments: ▪ The CSA Code is silent on this. Data may be transferred by an organisation out of Singapore. If control is retained within the organisation (e.g. transfer to a data bureau solely for processing and return to the organisation for use), the data remain subject to the operation of the Model Code. Comments: ▪ This is the position in UK. There is also the practical consideration that if data are not processed or controlled within Singapore, effective enforcement by any local oversight agency is precluded. ▪ On the issue of whether non-residents should be given the benefit of the protection under the Model Code, the consensus was that it was easier for businesses to comply with a broader "universal" scope as compared with distinguishing between people in Singapore and elsewhere. Another reason is so that the Model Code is consistent with the EU Directive in protecting the personal data of EU citizens and not merely Singapore citizens and Permanent Residents. (E.g. in Australia under the Privacy Act 1988, an Australian company may import data from European citizens and subsequently export them to a country with no privacy laws without the Australian regime applying. Such a measure would make it possible to circumvent the EU Directive if Australia was recognised as providing adequate protection. The Australian approach has thus been criticised by the EU.)

National Internet Advisory Committee ("NIAC") Model Code	Guidelines and Comments by the Legal Subcommittee of the NIAC
2. Definitions The following definitions apply in this Model Code: **Collection —** the act of gathering, acquiring, or obtaining personal data from any source, including third parties, by any means.	[Adapted from the CSA Code]
Consent — voluntary agreement with what is being done or proposed. Consent can be either express or implied. Express consent is given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the organisation seeking consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual.	[Adapted from the CSA Code] Comments: ▪ The Subcommittee is of the view that the best practice is for organisations to allow consumers to give consent through opt-in rather than opt-out procedures. (See also the comments at paragraph 4.3 on "Consent".)
Disclosure — making personal data available to others outside the organisation.	[Adapted from the CSA Code]
Organisation — a term used in the Model Code that includes associations, businesses, charitable organisations, clubs, institutions, professional practices, and unions.	[Adapted from the CSA Code] Comments: ▪ The Subcommittee is of the view that related organisations should be considered as separate organisations. Otherwise, disclosure within a large group of organisations will frustrate the objectives of the Model Code (e.g. a credit company disclosing personal information to an insurance company within the same group of companies). However, consent to disclose to related organisations may be implied (e.g. a request to purchase a car may imply the data subject's consent to the disclosure of his personal particulars to the car supplier for the purposes of the transaction).

National Internet Advisory Committee ("NIAC") Model Code	Guidelines and Comments by the Legal Subcommittee of the NIAC
Personal data — data, whether true or not, in an electronic form, which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.	[Adapted from UK Data Protection Act 1998] Individuals are identifiable not only by their names but also by their pictures, their telephone numbers, or by some special identification number (e.g. NRIC and Passport numbers), etc. "Personal data" means data which are in a form which can be understood by the recipient (e.g. encrypted data without the key would not be "information" because they cannot be understood). But they would become "information" (and hence "personal data") if they are capable of being decrypted. <u>Comments:</u> ▪ For the avoidance of doubt, the Subcommittee thinks that the Model Code should regulate personal information in the form of electronic data (i.e. "personal data" rather than "personal information"). ▪ See also the comments under paragraph 1.5. At a later stage, the Model Code may be extended to include manually-recorded personal data. In the meantime, organisations are free to subject their manually-recorded personal data to the operation of the Model Code.

National Internet Advisory Committee ("NIAC") Model Code	Guidelines and Comments by the Legal Subcommittee of the NIAC
	Comments: ▪ Another difficult area may arise in the context of b2b transactions. For example, if a business discloses, through one of its employees, its preference for products/supplies, is that personal information about the employee which should therefore be protected? The Subcommittee felt that only personal information purporting to relate to that employee personally would be considered "personal data". Data purporting to relate to a business would not normally be "identifiable" to that employee. The Subcommittee felt that such issues could be determined on the particular facts of each case.
Processing — any operation or set of operations which is performed upon personal data (whether or not by automatic means), 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.	Comments: ▪ The CSA did not define "processing". However, the Subcommittee felt a definition is necessary as the term is an integral concept in the Model Code. The definition is adopted from the EU Directive (Article 2).
Use — refers to the treatment and handling of personal data within an organisation.	[Adapted from the CSA Code]

National Internet Advisory Committee ("NIAC") Model Code	Guidelines and Comments by the Legal Subcommittee of the NIAC
3. General Requirements **3.1** The 11 principles that make up this Model Code are interrelated. Organisations adopting this Model Code shall adhere to the first 10 principles as a whole. Organisations which transfer personal data to third parties overseas should also adhere to Principle 11. Organisations may tailor this Model Code to meet their particular circumstances by (a) defining how they subscribe to the 11 principles; (b) developing an organisation-specific code; and (c) modifying the commentary to provide organisation-specific examples. **3.2** Each of the principles is followed by a commentary on the principle. The commentaries are intended to help individuals and organisations understand the significance and the implications of the principles. Where there is also a **note** following a principle (see principles 3 and 9), it forms an integral part of the principle. **3.3** Although the following clauses use prescriptive language (ie, the words "shall" or "must"), this Model Code is **voluntary**. Should an organisation choose to adopt the principles and general practices contained in this Model Code, the clauses containing prescriptive language become requirements. The use of the word "should" indicates a recommendation.	[Adapted from the CSA Code] Comments: ▪ Principle 11 is not in the CSA Code. However, the Subcommittee felt that the inclusion of Principle 11 is necessary for consistency with the EU Directive.

National Internet Advisory Committee ("NIAC") Model Code	**Guidelines and Comments by the Legal Subcommittee of the NIAC**
4. Principles **4.1 Principle 1 — Accountability** *An organisation is responsible for personal data under its control and shall designate an individual or individuals who are accountable for the organisation's compliance with the following principles.* **4.1.1** Accountability for the organisation's compliance with the principles rests with the designated individual(s), even though other individuals within the organisation may be responsible for the day-to-day collection and processing of personal data. In addition, other individuals within the organisation may be delegated to act on behalf of the designated individual(s). **4.1.2** The identity of the individual(s) designated by the organisation to oversee the organisation's compliance with the principles shall be made known upon request.	[Adapted from the CSA Code] Comments: ▪ This can be viewed in the context of the emerging prevalence in the US and EU of a position called the Chief Privacy Officer ('CPO'). This responsibility could also be assigned to the Chief Information Officer ('CIO') of the organisation or, in the absence of a CIO, to a member of the senior management. The CPO/CIO is responsible for the management and co-ordination of the information resources policies and procedures of the organisation. This position must have authority, and a voice that is heard by executive management. The CPO/CIO should have an in-depth knowledge of information management techniques, computer and telecommunications.

National Internet Advisory Committee ("NIAC") Model Code	Guidelines and Comments by the Legal Subcommittee of the NIAC
4.1.3 An organisation is responsible for personal data in its possession or custody. Where the data are to be transferred to a third party such that the organisation no longer has control over the data, the organisation should use contractual or other means to provide a comparable level of protection after the data are transferred to the third party. **4.1.4** Organisations shall implement policies and practices to give effect to the principles, including (a) implementing procedures to protect personal data; (b) establishing procedures to receive and respond to complaints and inquiries; (c) training staff and communicating to staff data about the organisation's policies and practices; and (d) developing data to explain the organisation's policies and procedures.	Generally, some responsibilities of the CPO/CIO are: • To establish and keep up-to-date information privacy policies and procedures; • To prepare privacy impact assessments of both current and proposed information systems; • To ensure the implementation of the organisation's privacy policies and practices by other organisations to which data processing functions are out-sourced. • To educate employees of the organisation on the importance of information protection; and • To stay abreast of technical and legal developments in this field in order to enable management to maintain the highest reasonable security standards. Other duties may arise, depending on the precise rights and remedies that may be created eventually by statute (if any). <u>Comments:</u> ▪ Concern was expressed by some members of the Subcommittee that complying with this principle, in particular 4.1.4 which they felt imposed onerous requirements, may entail significant cost to businesses. The majority however felt that this was an over-reaction and that procedures and identification of individuals responsible would not entail significant costs. Like IT security, data protection procedures and practices can be woven into the work processes of the organisation as good practices.

National Internet Advisory Committee ("NIAC") Model Code	Guidelines and Comments by the Legal Subcommittee of the NIAC
4.2 Principle 2 — Identifying Purposes *The purposes for which personal data are collected shall be identified by the organisation at or before the time the data are collected.* **4.2.1** The organisation shall document the purposes for which personal data are collected in order to comply with the Openness principle (Clause 4.8) and the Individual Access principle (Clause 4.9). **4.2.2** Identifying the purposes for which personal data are collected at or before the time of collection allows organisations to determine the data they need to collect to fulfil these purposes. The Limiting Collection principle (Clause 4.4) requires an organisation to collect only that data necessary for the purposes that have been identified.	[Adapted from CSA Code] Identifying purposes for the personal information to be collected forces organisations to focus their data collection on only information which is necessary for the stated purposes. This is critical to effectively limiting collection under Principle 4. This should not be viewed as a constraint on the organisation. Since data collection and maintenance may be costly, "identifying purposes" is the first step in reducing operating costs. Comments: ▪ Nonetheless, some concerns were raised that businesses may find it difficult to develop new uses of data if they have to determine from the very beginning every use that they intend for the data that they collect. This can however be overcome by an organisation by having a clear vision and far-sighted business plans.
4.2.3 The identified purposes should be specified at or before the time of collection to the individual from whom the personal data is collected. Depending upon the way in which the data are collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.	Comments: ▪ Members felt that extremely broad statements of purpose may make this principle nugatory (eg, an organisation could stipulate that it was collecting data "for your (i.e. the data subject's) benefit" or "to serve you better").

National Internet Advisory Committee ("NIAC") Model Code	**Guidelines and Comments by the Legal Subcommittee of the NIAC**
4.2.4 When personal data that have been collected are to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before data can be used for that purpose. For an elaboration on consent, please refer to the Consent principle (Clause 4.3).	Organisations may choose to adopt different consent regimes for different types of usage; usage on behalf of third parties; transfer to third parties, etc. However, the best practice is for organisations to give their consent through opt-in rather than opt-out procedures. (See also comments at paragraph 4.3.) Comments: ▪ On the issue of consent, the Subcommittee discussed current trends vis-à-vis "opt-in" or "opt-out" and noted that there was a marked movement towards the use of "opt-in" as opposed to "opt-out".
4.2.5 Persons collecting personal data should be able to explain to individuals the purposes for which the data are being collected. **4.2.6** This principle is linked closely to the Limiting Collection principle (Clause 4.4) and the Limiting Use, Disclosure, and Retention principle (Clause 4.5).	

National Internet Advisory Committee ("NIAC") Model Code	**Guidelines and Comments by the Legal Subcommittee of the NIAC**
4.3 Principle 3 — Consent *The knowledge and consent of the individual are required for the collection, use, or disclosure of personal data, save where the following exceptions apply:* *Collection without knowledge or consent of the individual is permitted where:* *(a) Collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;* *(b) Collection with the knowledge and consent of the individual would compromise the availability or the accuracy of the information where such collection pertains to an investigation of a breach of an agreement or the law; or* *(c) Collection is of data which is publicly available.* *Use without knowledge and consent of individual is permitted where:* *(d) Data is used in the investigation of an illegal act that has been, is being or is about to be committed;* *(e) Data is used in an emergency that threatens the life, health or security of an individual;* *(f) Use is of data which is publicly available; or* *(g) Use is of data for which consent for collection is exempted by either (a) or (b) above.* *Disclosure without knowledge or consent of the individual is permitted where:* *(h) Disclosure is made to a solicitor representing the organisation;* *(i) Disclosure is necessary for the purposes of establishing, exercising or defending legal rights;* *(j) Disclosure is to a government institution that has made a lawful request for the data;*	Informed or enlightened consent is the underpinning of fair information practices. Sometimes, the purpose for which data are collected is obvious and aligns so closely with the data subject's expectations that consent can be implied. Nonetheless, the subject has a right to what the principal purposes of the collection are, and whether there are any other intended purposes for the data. Therefore the application which the subject completes should identify the purposes. Notwithstanding, the list of purposes should not be so inclusive that individuals will not read or comprehend it. Consent can be obtained by any reasonable and convenient means, e.g. printed notices on applications, poster displays at entrances to premises, or on-line for internet transactions. In certain circumstances personal data can be collected, used, or disclosed without the knowledge and consent of the individual. These exceptions are set out in the Code. When data are being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the data. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organisations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organisation. In such cases, the organisation providing the list would be expected to obtain consent before disclosing personal data.

National Internet Advisory Committee ("NIAC") Model Code	Guidelines and Comments by the Legal Subcommittee of the NIAC
(k) Disclosure is made on the initiative of the organisation to an investigative body or a government institution; *(l) Disclosure is made to a person who needs the data because of an emergency that threatens the life, health or security of an individual;* *(m) Disclosure is made to an institution whose purpose is the conservation of records of historic or archival importance and disclosure is for such purpose;* *(n) Disclosure is made after the earlier of:* *- 100 years after the record was created; and* *- 20 years after the death of the data subject;* *(o) Disclosure is of data which is publicly available in that form; or* *(p) Disclosure is made by an investigative body and the disclosure is reasonable for purposes related to the investigation of a breach of an agreement or contravention of the law.*	Comments: ▪ According to the Implementation & Operational Guidelines on the CSA Code, prepared by the Canadian Information Processing Society (CIPS), internet "cookies" violate this principle. Although the browser informs the user that the web site is attempting to send a cookie (assuming of course that the browser has that capability), and the user can refuse to accept the cookie, this acceptance or rejection does not constitute consent, as the cookie notification does not contain any description of the use or uses of the cookie, who is collecting the information, etc.
4.3.1 Consent is required for the collection of personal data and the subsequent use or disclosure of this data. Typically, an organisation will seek consent for the use or disclosure of the data at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the data have been collected but before use (for example, when an organisation wants to use data for a purpose not previously identified).	Individuals should have the opportunity to opt out of data collection and to request deletion of that personal information which has already been collected. The individual may only be subjected to consequences because of this decision where the information is required to fulfil the explicitly specified, and legitimate purposes set out by the organisation (e.g. in the absence of the data on which to assess an individual's creditworthiness, an organisation may refuse to extend credit to him). Comments: ▪ While exceptions to the requirement of consent must be made explicit (see Art s 8.2, 8.3, 8.5 and 13 of the EU Directive, and s.3.2.6 of the Singapore Telecoms Competition Code), the Subcommittee felt that there was also a need to keep the Code "user-friendly" without overloading it with too much detail.
4.3.2 The principle requires "knowledge and consent". Organisations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the data will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the data will be used or disclosed.	Surreptitious data collection, except where explicitly permitted by law, contravenes the Model Code (e.g. collection of information by internet web sites about their client's interests —as inferred from the web sites visited —is unacceptable unless the clients are advised about the collection, and consent to it, prior to the collection taking place.) An unsuspecting public does not expect this data collection.

National Internet Advisory Committee ("NIAC") Model Code	**Guidelines and Comments by the Legal Subcommittee of the NIAC**
4.3.3 An organisation may not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of data beyond that required to fulfil the explicitly specified, and legitimate purposes.	Comments: ▪ The CPO/CIO may want to weigh the implications of using opt-out procedures very carefully, as the public may be averse to such procedures, which might be seen as analogous to reverse-marketing tactics (where the onus is on the individual to opt out of new services for which he might be charged). Nonetheless, the Subcommittee felt that opt-out procedures might still be acceptable, and even desirable, from the consumer's point of view, depending on the sensitivity of and intended uses for the personal data (e.g. own use vs. third party use, etc).
4.3.4 The form of the consent sought by the organisation may vary, depending upon the circumstances and the type of data. In determining the form of consent to use, organisations shall take into account the sensitivity of the data. Although some data (for example, medical records and income records) are almost always considered to be sensitive, any datum can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive data. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.	
4.3.5 In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organisation, in addition To using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organisation can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal data given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception or by providing misleading or incomplete information.	

National Internet Advisory Committee ("NIAC") Model Code	Guidelines and Comments by the Legal Subcommittee of the NIAC
4.3.6 The way in which an organisation seeks consent may vary, depending on the circumstances and the type of data collected. An organisation should generally seek express consent when the data are likely to be considered sensitive. Implied consent would generally be appropriate when the data are less sensitive. Consent can also be given by an authorised representative (such as a legal guardian or a person having power of attorney). **4.3.7** Individuals can give consent in many ways. For example: (a) an application form may be used to seek consent, collect data, and inform the individual of the use that will be made of the data. By completing and signing the form, the individual is giving consent to the collection and the specified uses; (b) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organisations. Individuals who do not check the box are assumed to consent to the transfer of this data to third parties; (c) consent may be given orally when data are collected over the telephone; or (d) consent may be given at the time that individuals use a product or service. **4.3.8** An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organisation should inform the individual of the implications of such withdrawal.	

National Internet Advisory Committee ("NIAC") Model Code	Guidelines and Comments by the Legal Subcommittee of the NIAC
4.4 Principle 4 — Limiting Collection *The collection of personal data shall be limited to that which is necessary for the purposes identified by the organisation. Data shall be collected by fair and lawful means.* **4.4.1** Organisations shall not collect personal data indiscriminately. Both the amount and the type of data collected shall be limited to that which is necessary to fulfil the purposes identified. Organisations should specify the type of data collected as part of their data-handling policies and practices, in accordance with the Openness principle (Clause 4.8). **4.4.2** The requirement that personal data be collected by fair and lawful means is intended to prevent organisations from collecting data by misleading or deceiving individuals about the purpose for which data are being collected. This requirement implies that consent with respect to collection must not be obtained through deception. **4.4.3** This principle is linked closely to the Identifying Purposes principle (Clause 4.2) and the Consent principle (Clause 4.3).	From a perspective of business efficacy, it is advantageous to collect only data which are necessary for a serious business purpose, as this translates into reduced costs for data collection and maintenance.

National Internet Advisory Committee ("NIAC") Model Code	Guidelines and Comments by the Legal Subcommittee of the NIAC
4.5 Principle 5 — Limiting Use, Disclosure, and Retention *Personal data shall not be used or disclosed for purposes other than those for which it was collected, except as provided by this Code or with the consent of the individual. Personal data shall be retained only as long as necessary for the fulfilment of those purposes.* **4.5.1** Organisations using personal data for a new purpose shall document this purpose (see Clause 4.2.1). **4.5.2** Organisations should develop guidelines and implement procedures with respect to the retention of personal data. These guidelines should include minimum and maximum retention periods. Personal data that have been used to make a decision about an individual shall be retained long enough to allow the individual access to the data after the decision has been made. An organisation may be subject to legislative requirements with respect to retention periods. **4.5.3** Personal data that are no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organisations should develop guidelines and implement procedures to govern the destruction of personal data. **4.5.4** This principle is closely linked to the Consent principle (Clause 4.3), the Identifying Purposes principle (Clause 4.2), and the Individual Access principle (Clause 4.9).	Access to personal data within an organisation must be allowed only on a need-to-know basis. Generally speaking, this should be based on a two-part test: • The employee must need access to the information in the performance of their duties; and • The access by the employee must be in support of a legitimate business function of the organisation. Data matching and data profiling activities are intrusive if the data sources for such activities are assembled for other purposes. The principle also deals with issues of records retention and destruction. Organisations should develop policies regarding the retention of records. This retention period must be long enough to allow individuals an opportunity to exercise their right of access under principle 9. Once this retention period expires, the information should be destroyed in a manner which prevents its re-creation.

National Internet Advisory Committee ("NIAC") Model Code	Guidelines and Comments by the Legal Subcommittee of the NIAC
4.6 Principle 6 — Accuracy *Personal data shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.* **4.6.1** The extent to which personal data shall be accurate, complete, and up-to-date will depend upon the use of the data, taking into account the interests of the individual. Data shall be sufficiently accurate, complete, and up-to-date to minimise the possibility that inappropriate data may be used to make a decision about the individual.	This principle reflects the relationship between data accuracy and the intended use of the information. Insofar as is possible, personal data should be collected directly from the data subject. This normally improves the quality of the information collected.
4.6.2 An organisation shall request updates of personal data from data subjects only where the update is necessary to fulfil the purposes for which the data were collected.	[Modified from the CSA Code, which is not so clear] The purpose of this principle is to prevent data collectors from routinely collecting updates of personal data needlessly, or on the pretext of regular updates.
4.6.3 Personal data that are used on an ongoing basis, including data that are disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.	
4.6.4 The organisation, in complying with this principle, may take into consideration the extent to which compliance is reasonable.	[Inserted by the Legal Subcommittee] Comments: ▪ It was felt that this should be expressly stated, as ensuring the accuracy of data may be costly.

National Internet Advisory Committee ("NIAC") Model Code	**Guidelines and Comments by the Legal Subcommittee of the NIAC**
4.7 Principle 7 — Safeguards *Personal data shall be protected by security safeguards appropriate to the sensitivity of the data.* **4.7.1** The security safeguards shall protect personal data against loss or theft, as well as unauthorised access, disclosure, copying, use, or modification. Organisations shall protect personal data regardless of the format in which they are held.	
4.7.2 The nature of the safeguards will vary depending on: - (a) the sensitivity of the data that have been collected; (b) the amount, distribution, and format of the data; (c) the method of storage; (d) the state of technological development; and (e) the cost and reasonableness of implementation of the safeguards. More sensitive data should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.	Security measures should be commensurate with the risks and consequences of disclosure. <u>Comments:</u> ▪ One commentator has expressed the following view: One safeguard that may be overlooked is deletion of data after the prescribed retention period. Personal data must be destroyed in a manner which prevents their re-creation. A normal file deletion does not meet this requirement since several utilities are available to restore it. It will be a good practice if the file is over-written at least three times or encrypted, or the media physically destroyed. Similar safeguards should be employed when personal computers are sent to suppliers for maintenance or when diskettes are used. Hardcopy files should be shredded.

National Internet Advisory Committee ("NIAC") Model Code	Guidelines and Comments by the Legal Subcommittee of the NIAC
4.7.3 The methods of protection should include (a) physical measures, for example, locked filing cabinets and restricted access to offices; (b) organisational measures, for example, security clearances and limiting access on a "need-to-know" basis; and (c) technological measures, for example, the use of passwords and encryption, as may be available, appropriate and reasonable from time to time. **4.7.4** Organisations shall make their employees aware of the importance of maintaining the confidentiality of personal data. **4.7.5** Care shall be used in the disposal or destruction of personal data, to prevent unauthorised parties from gaining access to the data (see Clause 4.5.3).	

National Internet Advisory Committee ("NIAC") Model Code	Guidelines and Comments by the Legal Subcommittee of the NIAC
4.8 Principle 8 — Openness *An organisation shall make readily available to individuals specific data about its policies and practices relating to the management of personal data.* **4.8.1** Organisations shall be open about their policies and practices with respect to the management of personal data. Individuals should be able to acquire data about an organisation's policies and practices without unreasonable effort. This data shall be made available in a form that is generally understandable. **4.8.2** The data made available shall include (a) the name/title and address of the person who is accountable for the organisation's policies and practices and to whom complaints or inquiries can be forwarded; (b) the means of gaining access to personal data held by the organisation; (c) a description of the type of personal data held by the organisation, including a general account of their use; (d) a copy of any brochures or other data that explain the organisation's policies, standards, or codes; and (e) what personal data are made available to related organisations (e.g. subsidiaries). **4.8.3** An organisation may make data on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organisation may choose to make brochures available in its place of business, mail data to its customers, provide online access, or establish a toll-free telephone number.	Comments: ▪ The Subcommittee's assessment was that this principle would not impose a great deal of cost to an organisation. On the other hand, it might be advantageous as it provides a competitive edge to the organisation. Internet web pages are very effective for disseminating such information. Where an organisation's "Privacy Policy" is displayed on its web site, translation (e.g. into the 4 official languages) is not necessary so long as the policy is set out in the same language medium as the web site itself.

National Internet Advisory Committee ("NIAC") Model Code	Guidelines and Comments by the Legal Subcommittee of the NIAC
4.9 Principle 9 — Individual Access and Correction *Subject to the following exceptions, an individual shall upon his request be informed of the existence, use, and disclosure of his personal data and shall be given access to that data. An individual shall be able to challenge the accuracy and completeness of his personal data and have them amended as appropriate. The reasons for denying access should be provided to the individual upon request.* *The organisation shall not provide access where:* *(a) Providing access would be likely to reveal personal data about a third party, unless* *- the third party consents to the access; or* *- an individual needs the information because an individual's life, health or security is threatened,* *provided that where the data about the third party is severable from the record containing the information about the individual, the organisation shall sever the information about the third party before giving the individual access; or* *(b) An investigative body or government institution, upon notice being given to it of the individual's request, objects to the organisation's complying with the request in respect of disclosures made to that investigative body or government institution;* *The organisation may refuse access where:* *(c) Data is protected by solicitor-client privilege;* *(d) It would reveal data that cannot be disclosed for public policy, legal, security, or commercial proprietory reasons;* *(e) It would threaten the life or security of another individual;* *(f) Data was collected under 4.3(b) (generally, collection pertaining to an investigation of a breach of an agreement or the law); or* *(g) It would be prohibitively costly to the organisation.*	Individuals have a right to access their personal data, and to know who has had access to it. When using email to provide for individual access, organisations should develop procedures for verifying the identity of the writer (i.e. that he is the data subject) before granting access. In certain situations, an organisation may not be able to provide access to all the personal data it holds about an individual. These exceptions are set out in the Code.

National Internet Advisory Committee ("NIAC") Model Code	Guidelines and Comments by the Legal Subcommittee of the NIAC
4.9.1 Upon request, an organisation shall inform an individual whether or not the organisation holds personal data about the individual. Organisations are encouraged to indicate the source of this data. The organisation shall allow the individual access to this data. However, the organisation may choose to make sensitive medical data available through a medical practitioner. In addition, the organisation should provide confirmation as to whether or not data relating to him are being processed and data at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed. **4.9.2** An individual may be required to provide sufficient data to permit an organisation to provide an account of the existence, use, and disclosure of personal data. The data provided shall only be used for this purpose. **4.9.3** In providing an account of third parties to which it has disclosed personal data about an individual, an organisation should attempt to be as specific as possible. When it is not possible to provide a list of the organisations to which it has actually disclosed data about an individual, the organisation should provide a list of organisations to which it may have disclosed data about the individual.	
4.9.4 An organisation shall respond to an individual's request for access within a reasonable time and without any excessive expense to the individual. The requested data shall be provided or made available in a form that is generally understandable. For example, if the organisation uses abbreviations or codes to record data, an explanation shall be provided.	[Modified from CSA Code] Comments: ▪ The CSA provides that the information must be provided at "*minimal or at no cost*" to the individual. The Subcommittee preferred the EU Directive's phrase: "*without excessive delay or expense*" (Article 12(a)).

National Internet Advisory Committee ("NIAC") Model Code	Guidelines and Comments by the Legal Subcommittee of the NIAC
4.9.5 When an individual successfully demonstrates the inaccuracy or incompleteness of personal data, the organisation shall amend the data as required within a reasonable time. Depending upon the nature of the data challenged, amendment involves the correction, deletion, or addition of data. Where appropriate, the amended data shall be transmitted to third parties having access to the data in question. **4.9.6** When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge should be recorded by the organisation. When appropriate, the existence of the unresolved challenge should be transmitted to third parties having access to the data in question.	The issue of who should bear the costs of correction is left silent. Organisations may develop their own policy. The best practice however is that such costs should not be passed on to consumers. Comments: ▪ The EU Directive is silent on the issue of rectification costs.

National Internet Advisory Committee ("NIAC") Model Code	**Guidelines and Comments by the Legal Subcommittee of the NIAC**
4.10 Principle 10 — Challenging Compliance *An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organisation's compliance.* **4.10.1** The individual accountable for an organisation's compliance is discussed in Clause 4.1.1. **4.10.2** Organisations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal data. The complaint process should be easily accessible and simple to use. **4.10.3** Organisations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint mechanisms. A range of these mechanisms may exist. For example, some regulatory bodies accept complaints about the personal data-handling practices of the companies that they regulate. **4.10.4** An organisation shall investigate all complaints. If a complaint is found to be justified through either the internal or external complaint review process, the organisation shall take appropriate measures, including, if necessary, amending its policies and practices.	Organisations are responsible for establishing a complaint receiving mechanism. Individuals should be advised, on the organisation's web site, how to submit complaints. Comments: ▪ The Subcommittee is of the view that this principle should be adopted flexibly in the light of the compliance mechanisms adopted by the organisations. A possible compliance mechanism might be for a certification body, such as the National Trust Council to adopt the code, e.g. as part of its good e-business practices under the TrustSg programme.

National Internet Advisory Committee ("NIAC") Model Code	Guidelines and Comments by the Legal Subcommittee of the NIAC
4.11 Principle 11 —Transborder Data Flows *An organisation may transfer personal data to someone (other than the organisation or the data subject) who is in a foreign country only if:* *(a) the organisation reasonably believes that the recipient of the data is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the data that are substantially similar to the data protection principles in this Code;* *(b) the data subject 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 pre-contractual measures taken in response to the data subject's request;* *(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the organisation and a third party;* *(e) all of the following apply:* *(i) the transfer is for the benefit of the data subject;* *(ii) it is impracticable to obtain the consent of the data subject to that transfer;* *(iii) if it were practicable to obtain such consent, the data subject would be likely to give it; or* *(f) the organisation has taken reasonable steps to ensure that the data which it has transferred will not be held, used or disclosed by the recipient of the data inconsistently with the data protection principles in this Code.*	[Adapted from Principle 9, Australian National Privacy Principles (Schedule 3, Privacy Act 1988)] Organisations that wish to export personal data should adopt this principle. Comments: ▪ This principle is not found in the CSA Code. However, it is arguable that this is a requirement under the EU Directive; data protection regimes which do not assure an adequate level of protection when exporting personal data may be considered inadequate by the EU. The restrictions on the onward transfers of personal data under this principle ensure that personal data enjoy similar levels of protection even when exported. Comments: ▪ This principle is based on the restrictions on international transfers of personal data set out in the EU Directive (Article 25).

National Internet Advisory Committee ("NIAC") Model Code	Guidelines and Comments by the Legal Subcommittee of the NIAC
5. Transitional Provisions Upon adoption of the Model Code, the Code applies to all personal data already in existence. However, the following principles shall only apply after a transition period of one year: (v) **Principle 6 (Accuracy) –** i.e. there would be no breach of this principle during the transition period; (vi) **Principle 9 (Access) –** i.e. the data user would not be required to provide a full copy of all data held at the time of the request, but would be entitled to first clean up the data by updating and removing irrelevant or dubious data. He would then be obliged to provide the data subject with a copy of all the remaining data.	Comments: ▪ The Subcommittee recognised that the adoption of the Model Code involves a major exercise by organisations in putting their data in order. It also requires the co-operation of data subjects in updating their data. Thus, the Subcommittee felt that it would be unfair to subject organisations immediately to the full force of the Model Code. ▪ On the other hand, the Subcommittee rejected the alternative position: that the Model Code should apply only to personal data generated after the Model Code is adopted by the organisation. This option was rejected on practical grounds and on principle. On practical grounds, it would be operationally difficult, if not impossible, to distinguish between data held before and after a particular date. On principle, the Subcommittee felt that it was unfair to permanently deny access and correction rights to existing data or to sanction the continued use or retention of data not collected or maintained in accordance with the principles. ▪ A good compromise between the 2 alternatives is for the Model Code to be implemented in phases, and for the provision of transitional provisions. Organisations may wish to modify the transitional periods according to the state of their records and their preparedness in meeting their new obligations under the Model Code. This flexibility allows organisations to adopt the Model Code in phases, at a pace sustainable according to their particular needs. If these transitional provisions (with or without modifications as to the transitional period) are adopted by the organisation, a notice to this effect should be clearly set out in its Privacy Policy, in order not to mislead the public.

ANNEX 5

COMPARATIVE TABLE FOR DEFINITIONS OF PERSONAL DATA ("P.D.") / PERSONAL INFORMATION ("P.I.")

OECD	EU Directive	UK	Canada			New Zealand	Australia	Hong Kong	NIAC Code
			CSA Code	Privacy Act	PIPEDA				
"p.d." means any info relating to an identified or identifiable individual ('data subject')	"p.d." means any info relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.	"p.d." means data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other info which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. ["data" is defined and includes automatically processed or processible info as well as data falling within the definition of a "relevant filing system" (manual data).]	"p.i." means info about an identifiable individual that is recorded in any form	"p.i." means info about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing, [(a) - (m) which sets out particular instances of p.i.]	"p.i." means info about an identifiable individual, but does not include the names, title or business address or telephone no. of an employee of an organisation	"p.i." means info about an identifiable individual, and includes info contained in any register of deaths kept under the BDR Act. ["individual" is defined as a natural person, other than a deceased natural person.]	"p.i." means info or an opinion (including info or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the info or opinion.	"p.d." means any data (a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable. ["data" is defined as "any representation of information (including an expression of opinion) in any document, and includes a personal identifier"]	"p.d." means data, whether true or not, recorded in an electronic form, which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other info which is in the possession of, or is likely to come into the possession of, the data controller.

OECD = OECD Guidelines on the Protection of Personal Data (1980)
EU = EU Directive on the Protection of Personal Information (1995)
UK = UK Data Protection Act 1998
NZ = Privacy Act 1993
AUS = Privacy Act 1988 incorp'g Privacy Act (Private Sector) Amendment Act 2000
HK = Personal Data (Privacy) Ordinance 1995, Cap. 486