WORKING PAPER 1

# DATA PROTECTION IN SINGAPORE

*A Case for Legislation*

INTRODUCTION

1. The Sub-Committee for Technology & Law is part of the Law Reform Committee, Singapore Academy of Law.[1] Its role is to consider the legal aspects of technology and to make recommendations where appropriate. In recent years, the most profound technological changes have been in information technology. The Committee has therefore concentrated on this and has identified the following areas for study during its term of office:

—Data Protection

—Computer Misuse

—Computer Output as Evidence

2. The intention of this paper is to define and discuss the issues and to present proposals for consideration by interested parties. In particular, the issue to be examined is whether legislation is desirable in this area and if so, what form it ought to take. It is important to note at this point that the issues of data protection are related to, but distinct from, those involving computer misuse. Laws on data protection have as their primary aim the protection of "personal information". Such protection usually takes the form of restricting the transfer of information among data users, both nationally and internationally. Legal rights are usually given to data subjects to remedy any misuse of data by the data users. Laws against computer misuse are usually criminal in nature and have as their main aim the punishment of offenders who misuse computers either for profit or for gratuitous diversion. These laws therefore are discrete but complementary.

3. The use of computers to store and process data is now commonplace in Singapore. The collection and processing of personal information is on the increase as is the impetus for networking, both nationally and internationally.[2] In the midst of the technological progress, the interests of data subjects should not be ignored. Data users possess vast amounts of data about individuals and institutions, frequently of a

sensitive nature. The information may be quickly retrieved either in the form in which it is entered or processed with other data to form another, perhaps more thorough, picture of the data subject. The risks of unauthorised disclosure and abuse are manifold – such disclosure may cause economic loss, emotional distress or even physical harm. Now, any data subject who is aggrieved has to rely on existing legal remedies that may be inadequate or inappropriate.

4. Singapore's national policy to promote the use of information technology should be accompanied by modern rules and regulations so that information technology developments can take place under controlled conditions. The pace of technological change in general and information technology in particular, has usually outstripped legal change. While this may be expected and tolerated, the law ought not to lag too far behind.

5. The Australian Law Reform Commission recently completed an impressive general study of Privacy.[3] The Report identified nine sources of concern created by the informatics industry – *Amount, Speed, Cost, Linkages, Profiles, New Profession, Accessibility, Centralization, International.*[4] According to the Commission, the increase in storage and processing power coupled with reducing costs of hardware and software all make for the ease with which information can be stored, processed and used. Standardization of communication protocols also enable the widespread exchange of data, whether domestically or internationally.

6. An important concern is the ability of computers to link disparate data to form composite profiles of data subjects. The proliferation of information systems also means that there is a corresponding growth in the number of professionals. Unlike the well-established professions the doctors, lawyers, accountants and engineers no general disciplinary body exists to control computer professionals. Neither is there a code of conduct laying down general principles and norms of good behaviour. In many jurisdictions, particularly the Western ones,[5] these concerns have led to legislation. Internationally, the Council of Europe and the Council of the OECD have been in the forefront in setting the policies and standards for national legislation.[6] Most data protection legislation adopt, *mutadis mutandis*, the principles set out in the guidelines provided by these two institutions. The Sub-Committee's view is that these international guidelines are useful in determining the framework for legislation in Singapore.

## Reasons for legislation

### PROTECTION OF DATA SUBJECTS

7. There is little doubt that the main motive for data protection or privacy legislation is the need to protect the interests of individual data subjects. Privacy is perceived as a fundamental right deserving legal protection. Privacy laws have been justified on cultural, psychological and religious grounds. Privacy laws may also serve the practical function of ensuring that data collected for one purpose be prevented from being used for another less suitable purpose and thus avoiding policies that may be based on misleading data.[7] The protection also may extend across national boundaries.[8]

8. The information services market is also growing. Public sector bodies are being regarded more and more as major producers of basic information and data which they collect routinely, not just from the people but also from other institutions such as banks and public companies. The public sector is seen as having the potential to be a strong provider of information goods and services. At the same time, there must be some thought paid to the extent to which such information may be distributed to other data users. In addition to rules protecting information concerning national security and affairs of state, the protection of personal data and similar information should be provided. In other words, the regulation of the public sector's use and distribution of information of all types, should be explicitly provided for in legislation.

### PROVISION OF STANDARDS FOR DATA USERS

9. The growth of the informatics industry brings with it a new profession data users and their staff. Information given in confidence by data subjects is handled daily by operators who are not subject to any general code of conduct similar to those imposed on engineers, lawyers, doctors and accountants. The diversity of functions and personnel adds to the problem: who or what level of computer operators should be subject to codes of conduct?[9]

10. Besides the problem of operator responsibility, today's technology enables data users to hide information through security measures such as passwords, encryption and the like. Where there is no duty to disclose such information or a duty to verify or correct data, data subjects may be prejudiced by data that may be incorrectly entered, or corrupted while being processed or retrieved. Decision-makers relying on inaccurate data may come to the wrong conclusions.

## CONFORMITY WITH INTERNATIONAL STANDARDS

11. The growth of the informatics industry is fuelled by the ease with which data links can be established across national boundaries. Transborder data flows are now commonplace and increasing. Also evident is the recognition especially by European countries of the dangers attendant to transborder data flows of personal data. All European legislation, whether enacted or prospective, provide restrictions on transborder data flows unless the recipient country also has legislation that protect the rights of data subjects.

12. The three reasons given are sufficient to justify legislative action of some sort. It must not be thought still that there are no countervailing interests that may affect the issue whether there ought to be such legislation. A duty to disclose information for instance may in appropriate circumstances adversely affect criminal investigations, or economic relations or national security. In the private sector, the protection of financial resources and assets and the protection of managerial effectiveness and efficacy are interests that may restrict the scope of data protection laws. The existence of such interests means that the function of a data protection law–

*should [be to] provide a framework for finding a balance between the interests of the individual, the data user and the community at large.*[10]

# Basic Ideas

## *DATA, INFORMATION AND PRIVACY*

13. Data itself is an amorphous word, usually referring to information that is in a processable form.[11] This is narrower than the word information that may cover all forms of recognizable fact and opinion. The legal protection of information in its widest sense is beyond the scope of any single piece of legislation. It may involve constitutional or public law or criminal law besides private law remedies. The criminal law, for instance, is used to protect information criminal defamation, unauthorised disclosure of confidential information and so on.[12] The protection of information as distinct from data may involve freedom of information legislation. Such legislation usually confers on individuals the right to disclosure of information kept in the public sector.[13] An extensive law on information is not within the purview of this Sub-Committee. The reasons justifying freedom of information legislation primarily based on open government are not the same as those justifying data protection laws. Even countries with extensive

privacy laws like Australia have provided for freedom of information legislation in a separate legal instrument.[14]

14. Where there is specific data protection legislation, it normally protects personal data. The addition of personal to the word is an important qualification and distinguishes it from laws on freedom of information and privacy. Privacy is a wider concept, involving three separate elements: secrecy, anonymity, solitude.[15] Thus, a law on privacy would cover not only misuse of information provided by individuals but also physical intrusions (arrest, search and seizure powers, covert surveillance etc..). Data protection is normally referred to as informational privacy and is a subset of rules protecting privacy generally. Territorial privacy and privacy of the person are protected by the criminal law and procedure and by the law of torts.

*PERSONAL DATA*

15. An important concept in determining the scope of data protection legislation is personal data or personal information. Statutory definitions of this vital concept are varied. For example, the Australian definition defines personal information as information about a natural person from which, or by the use of which, the person can be identified.[16] The Canadian Privacy Act 1982 prefers to spell out the types of personal information. The formula includes–

- information relating to race, national or ethnic origin, colour, religion, age or marital status;
- information relating to the education, medical, criminal or employment history and information on his financial transactions;
- any identifying number, symbol or other particular assigned to the individual;
- the address, fingerprints or blood type of the individual;
- records of the personal opinions of the individual;
- confidential correspondence;
- confidential views or opinions of others about the individual.[17]

16. In defining what personal information ought to cover, one important issue is whether it ought to include legal persons, that is, corporations and societies. Some countries do include legal persons in their legislation: Austria, Denmark and France. Others take the view that it is enough to protect natural persons Australia, UK, Ireland. Several reasons may be given for restricting the legislation to natural or living persons. First, the laws relating to business are very different from those relating to individuals.. The laws on restraint of trade, copyright and patents are based on policy concerning

business competition. Secondly, if corporations were included, they may see such legislation as a means to finding out what their rivals know about them. This potential abuse to data protection law would detract from its main purpose, namely to protect the interests of data subjects rather than to provide a weapon for business institutions. Third, there is the fear that including corporations in data protection legislation may make the scheme too large and unmanageable. It may also be unnecessary. If a data protection law includes corporate entities, attention may be diverted from the policies underlying the protection of information about natural persons. For these reasons, therefore, the approach of the Sub-Committee is to restrict its view of personal information to information on natural or living persons only.

*DATA PROTECTION*

17. This open-ended phrase means different things to different people. Data users[18] may identify the phrase with the need to keep data secure from unauthorized use or disclosure. Data subjects may regard such a phrase as concerning rights to the information kept about them by the data users. For the purposes of this Paper, it is from the viewpoint of the data subjects that the Sub-Committee is concerned. In other words, a data protection law has as its primary objective the protection of the data subjects from the misuse of information collected about him by data users, both in the public and private sectors.

## The Present Legal Framework in Singapore[19]

18. The existing legal controls in the protection of personal information are not computer-specific. They were evolved when the informatics industry was either non-existent or insignificant. For instance, there are no laws at this time dealing with electronic breaking and entering. The availability of criminal or civil sanctions against misuse of personal information are affected by civil and criminal procedural rules that may hinder success. The Sub-Committee is of the view that existing law is not adequate to meet the growth experienced in the informatics industry.

*LEGISLATION*

19. The existing legislation protecting the disclosure of personal information is primarily in the public sector. It is not computer-specific and applies to all types of records whether kept in computers or other means. Statutes with sanctions for dealing with improper disclosure of information by public servants include–

—Official Secrets Act (Cap 213);[20]

—Telecommunications Authority of Singapore Act (Cap 323);

—Monetary Authority of Singapore Act (Cap 186);

—Statutory Bodies & Government Companies (Protection of Secrecy) Act (Cap 319).

20. Typically, these statutes provide for criminal sanctions in the event of unauthorised disclosure of confidential information. Where a public officer is under the Official Secrets Act, he may also be liable if he did not take reasonable care to secure information.[21]

21. In the private sector, there is little by way of legislation imposing sanctions for disclosure of information. The primary example is the Banking Act (Cap 19) that protects information relating to money or other relevant particulars of customers and their accounts.[22]

*COMMON-LAW*

22. At common-law, protection for personal information may depend on whether there is a contractual relationship between the data subject and the unauthorised user. If a contract does not exist, the remedies may lie in the law of torts or restitution. It may be added that common-law remedies appear to be the main recourse in the private sector.

*Actions in contract*

23. Where there is a term in the contract, either express or implied, to prevent a party or his agents from disclosing confidential information, an action for breach may be sustained. Damages may be recoverable or where appropriate, an injunction preventing the disclosure. One writer has suggested that the best way to protect personal information is by way of an express term that there should be no disclosure except with the written consent of the subject.[23]

24. Yet, the law of contract may not be adequate for several reasons: first, the prevalence of standard form contracts may preclude the inclusion of terms concerning confidential information. Second, the law of contract is developed with a view to compensating loss. It is not particularly suited as a preventive device. Also, disclosure of information may cause not just financial loss but emotional distress and the like. The law of contract frowns on recovery for mental distress. Finally, there may be no way to stop one party, especially the dominant party, from the use of exclusion clauses to escape liability.

*Breach of Confidence*

25. The common-law provides that a supplier of confidential information may obtain an injunction to stop another from wrongfully disclosing confidential information. But, three conditions must be satisfied: first, the information must be of a confidential

nature; secondly, there must be a duty to keep such information confidential; thirdly, there must have been a breach of this duty. Finally, the plaintiff must show that there was unauthorised use to the detriment of the owner of the information. The success of this type of action depends on whether the party knows about the potential breach and takes action quickly enough to prevent it. There is no scope for the remedy once the information is made public.[24] The costs of legal action may also be a deterrence to action by the aggrieved party, especially where the information may be viewed to be somewhat trivial.

*Other civil remedies*

26. The law of torts does compensate for mental distress and physical loss. But, again, it is compensatory in nature. There is also no development of a tort of privacy similar to that evolved by the US courts. Under the US doctrine, an unreasonable invasion of privacy (such as undue publicity about the private life) of the plaintiff can give rise to a cause of action. In Singapore, a plaintiff may have to base his action in negligence or trespass to goods (e.g., in the case of unauthorised access to a database). Collusion between the data users' employees and outside parties may be evidence of a conspiracy though it is necessary even in such a case to prove that there is an intention to cause harm to the employer. If a third party induces an employee to disclose information contrary to the terms of the employment contract, there may be a cause of action based on inducing breach of contract. Finally, disclosure or use of information that is inaccurate or incomplete may give rise to actions in negligence or defamation. Disclosures may also be prevented by the law relating to State privilege or legal professional privilege.[25]

## The Overseas Experience

*INTERNATIONAL GUIDELINES*

27. The international scene has been dominated by two international instruments providing guidelines for national legislation. These are the OECD Guidelines on the Protection of Privacy & Transborder Data Flows of Personal Data[26] and the Council of Europe Convention (Treaty 108).[27] Although the guidelines are not obligatory even for member states of the OECD, almost all the countries have expressly in their national legislation embraced the principles. These guidelines must therefore be the starting point for any proposals. Recently, the United Nations has published similar draft guidelines for consideration by member states.[28]

*OECD BASIC PRINCIPLES OF NATIONAL APPLICATION*

28. The Guidelines were drafted to balance the competing interests between protecting privacy and promoting a free flow of information. The Preamble to the Guidelines recognises that transborder data flows of personal data may contribute to economic and social development and that such flows could be hindered by domestic data protection legislation. Countries are encouraged to avoid placing unnecessary obstacles to the free flow of information.

29. There are eight basic principles that can be classified according to the information processing cycle – collection, storage, use and disclosure.

COLLECTION LIMITATION PRINCIPLE

*There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge and consent of the data subject.*

DATA QUALITY PRINCIPLE

*Personal data should be relevant to the purposes for which they are used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.*

PURPOSE SPECIFICATION PRINCIPLE

*The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change or purpose.*

30. These three principles are primarily about the data collection stage. The principles impose duties on data collectors one, that they must obtain their data lawfully and fairly; two, that they must be clear about the purpose or purposes for which the data is obtained and three, that the data so collected is properly stored and updated. The data subject should know of the purpose for which the data is collected before such information is given.

USE LIMITATION PRINCIPLE

*Personal data should not be disclosed, made available or otherwise used for the purposes other than those specified in accordance with [the Purpose Specification Principle] except*

*— with the consent of the data subject; or*

*—by the authority of law.*

SECURITY SAFEGUARDS PRINCIPLE

*Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.*

31. The Use Limitation Principle may indirectly prohibit most data users from sale of the database. This is because very few people are likely to give personal data freely so that another party may profit from the sale of it. The exceptions are important either there should be express legislation requiring the disclosure or the data subject's consent must be obtained. The demands placed on data users by the Security Safeguards Principle are fairly obvious. Security measures are essential to the integrity of the data users' systems and it would be an imprudent (probably negligent) data user indeed who would not implement security measures in his information system.

OPENNESS PRINCIPLE

*There should be a general policy of openness about developments, practice and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data and the main purposes of their use as well as the identity and usual residence of the data controller.*

32. This principle and the one below form the basis of the rights of data subjects. Without the Openness Principle that would allow data subjects to identify data users and the data, the rights to challenge and change data would be illusory.

INDIVIDUAL PARTICIPATION PRINCIPLE

*An individual should have the right–*

(a) *to obtain from a data controller or otherwise, confirmation of whether or not the data controller has data relating to him;*

(b) *to have communicated to him, data relating to him–*

*(i) within a reasonable time;*

*(ii) at a charge, if any, that is not excessive;*

*(iii) in a reasonable manner; and*

*(iv) in a form that is readily intelligible to him;*

*(c) to be given reasons if a request made under sub- paragraphs (a) and (b) is denied, and to be able to challenge such denial; and*

*(d) to challenge data relating to him and if the challenge is successful, to have the data erased, rectified, completed or amended.*

33. With the Openness Principle, this Principle will confer meaningful rights to data subjects. But, it strikes a balance between the right to know and the cost of knowledge

because the Principle does allow for the data users to impose a reasonable charge for providing the information. The cluster of rights which this Principle entails will generally ensure that information kept in databases is accurate and updated regularly.

ACCOUNTABILITY PRINCIPLE

*A data controller should be accountable for complying with measures that give effect to the principles stated above.*

34. Without enforcement machinery, the rights conferred on individual data subjects would be illusory. It is a matter of national policy how stringent the measures should be to get a satisfactory level of compliance.

*THE COUNCIL OF EUROPE CONVENTION*

35. The Convention was opened for ratification in January 1981 and came into force on October 1, 1985. Ratification of the Convention can only take place after a state has enacted domestic legislation taking into account the principles embodied in the Convention.[29]

36. The Convention is directed primarily at controlling automated personal data files and automatic processing of personal data in both the public and private sectors. Article 6 restricts the processing of certain types of data. The Article states–

*Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides adequate safeguards. The same shall apply to personal data relating to criminal convictions.*

37. This Article envisages that sensitive data requires special consideration. Further it identifies the types of sensitive data that ought to be specially provided for. The question as to what is sensitive must necessarily differ from country to country. For example, Singaporeans may not find data revealing their racial origin to be particularly sensitive. At the same time, they would probably regard data about their financial assets and liabilities as of great sensitivity.

38. The Convention also provides for the extent to which data users may be exempt from the requirements of data protection laws. The derogation from such principles is permissible when it is –

*provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:*

*– protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;*

– *protecting the data subject of the rights and freedoms of others.*[30]

39. The Convention thus explicitly recognises the countervailing interests that may limit the rights of data subjects. These limits may mean that there can be no right of disclosure with respect to certain databases, for example, those involving the cataloguing of evidence of crimes. It would be dangerous indeed if a suspect can require information about witnesses' names by exercising his right to know the nature of the case against him. The provision of these exceptions to data protection obligations appear quite broad. It is up to the good sense of the government and other institutions to apply the spirit of the Convention and not to provide for too many categories of exemptions.

*THE UN GUIDELINES*

40. The United Nations have released a draft set of Guidelines on Computerised Personal Data Files.[31] These are expected to be approved by the General Assembly in due course. There are eleven Articles and six Principles with ancillary provisions. Although the Guidelines follow the OECD Guidelines, they are more specific in what ought not to be done. For example, the Principle of Non-Discrimination provides that–

*data likely to give rise to unlawful or arbitrary discrimination, especially information on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical beliefs as well as membership of an association or a trade union, should not be compiled.*

41. There is some similarity between this Principle and that contained in Article 6 of the Convention. It is wider than the latter in including membership of trade unions. But, it may be asked whether this is not unduly excessive even a trade union would not be able to computerise its membership lists under this Principle. It is submitted that the key lies in the opening words data likely to give rise to unlawful discrimination. Whether a database would fall foul of this Principle then depends on how the information in it is used.

42. There is also an exceptions clause in the UN Guidelines. Personal data need not be disclosed where the interests of national security, public health, public order or morality are likely to be prejudiced by such disclosure. But, such exceptions must be provided for in legislation and limits and safeguards specified.

43. In terms of enforcement machinery, the UN Guidelines are more specific. By Article 8, it is provided that–

*the law of every country shall designate the authority that, according to its domestic legal system, is to be responsible for supervising observance of the principles set forth above. This author-*

*ity shall offer guarantees of impartiality and technical competence. In the event of violation of the provisions of the national law implementing the aforementioned principles, criminal penalties should be envisaged together with the appropriate remedies.*

44. This Article is useful in that it clearly sets out the nature of the enforcement and monitoring institutions that first, it must be independent (presumably of all interested parties in both the public and private sectors) and secondly, that it must have the necessary technical expertise. Finally, there is very little to quarrel with the proposition that any data protection law must be backed up by criminal sanctions together with remedies for data subjects.

45. These three international instruments provide useful guides to the drafting of national legislation. But, it would be prudent to look also at the nature of existing national legislation: the aim here is to find the common features. It is not intended to comment separately on the variety of provisions and techniques involved in each country's legislation.[32]

*NATIONAL LEGISLATION*

46. Legislation at the national level is so diverse in terms of content and institutions that it would be beyond the scope of this Paper to examine the thirty or so models.[33] Some countries such as Sweden feel so strongly about the matter that they have introduced amendments at the constitutional level to reflect the importance of data protection rights. Thus, the Swedish constitutional document the Instrument of Government has been recently amended to include the provision that –

*Every citizen shall to the extent more precisely laid down by law be protected against infringements of his personal privacy by recording information about him by automatic data processing.*[34]

47. On the other hand, national or state governments may prefer to be cautious and just implement guidelines while legislation is being considered, e.g., Hong Kong.[35]

48. When examining common features, certain key issues may be identified. These are–

**(1) whether there ought to be legislation or whether the public and private sectors ought to be self-regulating?**

**(2) whether legislation or rules should apply to all forms of records, manual or automatic?**

**(3) what are the institutions required to ensure that data protection laws are effective?**

**(4) who or what should be exempted from the obligations of data protection laws?**

SCOPE OF DATA PROTECTION: BLANKET OR SECTORIAL APPROACH?

49. One difference in legislative scope is that some countries prefer to enact one statute to cover all sectors, e.g., UK, France whereas other countries have different instruments for different sectors. Usually, the distinction is between the public and private sectors. The US, Canada and Japan for example have legislation governing the public sector but not the private sector. Given the diversity of automatic processing, both in terms of content and methods, it is now more common to find a general statute providing only general principles similar to those in the international instruments. The general statute is buttressed by subsidiary legislation or codes of conduct that are sectorial in nature. In this way, the law can move with technological change. Codes of conduct can respond to changes quicker.

SCOPE OF LEGISLATION – MANUAL OR AUTOMATIC PROCESSING?

50. Countries like France, Germany, Denmark, Norway regard manual records in the same way as automatically processed ones and apply the same rules. However, such an approach usually increase the administration costs tremendously as the registration and monitoring tasks will be quite immense. The arguments for including manual records are that the same dangers of misuse are present; that if there is a distinction made between manual and automatic records, there will be difficulty classifying hybrid systems.[36] At some stage, there is probably some manual data handling, e.g., filling in an application form or a questionnaire. Third, the exemption of manual record systems may lead to data users evading the data protection laws by not automating their records systems. While there is substance in these arguments, it must be balanced against the costs. Not only will the administration be expensive but also inconvenient. It is also expected that given the obvious advantages of automatic processing, data users will want to avoid it just to evade data processing regulations. On balance, it is probably preferable to restrict laws to automatic processing where the dangers are perceived to be the greatest. In contrast, manual records or paper files are less prone to unauthorised manipulation as the perpetrators have to gain physical access to such files.

## SCOPE OF LEGISLATION: CATEGORIES OF PERSONAL DATA

51. Paragraphs 13 and 14 above already refer to the problems of defining what is personal data. It is pertinent to note that a data protection law that attempts to cover all types of personal data may be difficult to implement. Neither is it necessary for certain personal data may be of low sensitivity. Low sensitivity data such as telephone numbers and addresses that are listed in a telephone directory may not cause much concern as such data can hardly be said to be confidential.[37] As the sensitivity of data increases, so must the protection. Certain legislation like the Irish Data Protection Act 1988 only requires registration for those data users dealing with the restricted categories of data mentioned in the Convention. Thus data controllers keeping data on racial origins, political opinions, religious beliefs, health etc.. would have to register.

52. It may be possible to examine the various categories of personal data and to determine the degree of sensitivity. Data subjects who disagree with a general classification may, as is true of a telephone subscriber, inform data users of their special sensitivities and have such information removed from the database. Of course, data users of personal data may still be under the obligations imposed by a data protection law. But, as in the Irish Act, the nature of obligations may differ according to the sensitivity of information kept.

## IMPLEMENTATION: CONTROL INSTITUTIONS

53. The international instruments all envisage data protection authorities to have a certain measure of autonomy. In practice, however, there is as expected, wide differences as to how independent a data protection authority must be. In theory, the data protection authority has to protect the interests of the data subjects against both public sector data users as well as private sector data users. Complete autonomy may involve a person such as an Ombudsman, as in the Finnish model. At the other end, the Japanese data protection authority is part of the Prime Minister's Office.[38] By and large, Western nations are more concerned with the independence of the data protection authority. This is expected as the traditions of the separation of powers are better observed. In many cases, the rights of data subjects are buttressed with further rights of appeal to quasi-judicial tribunals. Of course, recourse may be had to the courts if data subjects prefer to invoke the full weight of the law.

IMPLEMENTATION: LEGISLATION OR VOLUNTARY CODES OF CONDUCT?

54. As described in the preceding paragraphs, many countries have opted for legislation. Voluntary codes of conduct are seen to be interim measures which are brought in to fill the gap while legislation is being prepared.[39] Other countries such as Japan may legislate only for one sector usually the public sector and leave the private sector to provide their own codes of conduct. Such a solution is not common in the European countries. Codes of conduct such as those in the UK are made under the aegis of the legislation. It was felt that voluntary codes of conduct would not be adhered to by those for whom such guidelines are intended. Sanctions can only be imposed by legislation and for the codes of conduct to be effective, they must be supported by legislation.

IMPLEMENTATION - EXEMPTIONS

55. All the data protection legislation and international instruments provide exemptions for certain data users from all or some of the obligations. Exemptions may be defended on several grounds:

- no natural person can be identified from the stored data;
- disclosure may prejudice national security or national economic interests;
- the data may concern only trivial matters such as domestic records or recreational activities;
- disclosure may prejudice the data subject.

56. Most countries recognise that there must be some exemptions from disclosure. State interests may in certain circumstances prevail over individual rights disclosing information on tax evasion to the suspect may hinder criminal investigations. Where medical information is concerned, disclosure of such information may cause shock or mental distress to the patient. The data user probably the medical practitioner in this example may have to have residual powers to refuse disclosure. Such residual powers must be defined with some care and must not become the route for data users to escape responsibility. At the same time, such detailed exemptions should ideally not be in legislation but in codes of conduct which are made under the aegis of legislation.

57. Existing national legislation therefore shows great diversity both in content and technique. All purport to comply with the OECD Guidelines. The models range from the minimal ones like the Japanese model (restricted to public sector and accountable to the PM) to wide or maximalist models such as the Australian Privacy Act. Compliance

with the OECD principles then may be flexible although one must not lose sight of the general aim of data protection, which is, the protection of data users.

**[Part II - Options for Singapore - follows this page]**

# PART II

# OPTIONS FOR SINGAPORE

*GENERAL CONSIDERATIONS*

58. The reasons for legislation are discussed above in paragraphs 7-12. Here, in making proposals, the Sub-Committee is conscious that data protection is a relatively new concept even in the West. New legal rights for data users are created by legislation and are not normally within the contemplation of data subjects. It may therefore be thought that such laws are unnecessary– the people do not expect them and there is no demand for them. At the same time, enactment may restrict data users' freedom to use information, and may cause needless inconvenience to all parties. It may also be asserted that data protection laws may arrest the growth of the database industry.

59. The Sub-Committee recognises these arguments but is of the view that whatever the short-term benefits of non-action, it is not in Singapore's long- term interests if it wants to succeed as a world class exploiter and provider of IT products and services.[40] For the existing data protection legislation of all countries do provide for restrictions to transborder data flows to countries without reciprocal legislation.[41] The Sub-Committee submits that globalization of the informatics industry require conformity to international conventions. Further, a desire to protect information and more importantly, data subjects, demonstrates the maturity of the industry and country. Rules to govern data collection, use and disclosure comprise the heart of standards for governing the conduct of computer professionals.

60. Another argument is that such legislation may hinder data sharing and consequently reduces the value of computerisation. Certain countries, notably the major Western democracies, have legislation or guidelines preventing the cross-matching of data particularly in the public sector. There is a dislike, even repugnance, for government agencies having too much information about individuals. This issue is examined further below.

*LEGISLATION FOR PUBLIC & PRIVATE SECTORS?*

61. The Sub-Committee first considered whether, if there is a case for data protection legislation, it should cover both the public and private sectors.

62. Having offered reasons for legislation above, the Sub- Committee considered the various options available for a data protection law. These are:

**(a) No legislative action rely on existing law;**

**(b) Voluntary codes of conduct in all sectors;**

**(c) Mandatory rules (legislation) in the public sector; voluntary codes in the private sector;**

**(d) Mandatory rules (legislation) in the private sector; voluntary codes in the public sector;**

**(e) Mandatory rules (legislation) for all sectors.**

63. As explained in paragraphs 18-26, existing legal remedies are inappropriate or inadequate for the problems concerning automated databases, the main problem being that there is usually no right of access to check and amend data (unless the data subject makes it a term of the contract). Option (a) retaining the status quo is only acceptable if data protection is not seen as being of benefit to the country.

64. The main limitation to the use of voluntary codes (Option b) is that they are at most stop-gap measures. As a learned author puts it,

*"The danger is that any voluntary agreement will be subscribed to and carried out by those for whom it is least necessary, and either evaded or ignored by the others."*42

65. As the experience of other countries have shown, the more accepted approach is legislation. Some only legislate for the public sector and allow the private sector to be self-regulatory. This is the approach being tried out in Japan, for example. But the Sub-Committee perceives that this is unsatisfactory because a large sector would be left to self-regulation and in the view of the members, this attracts the same criticism as option 2, namely that self- regulation on such matters is no better than no regulation at all. Furthermore, legislating on the public sector alone may give the wrong signal to all concerned, that only the public sector needed to be controlled and that private industry can do whatever it likes with similar data. Finally, it is noticeable that the public sector is very conscious of the need for security and protection of data. It is governed extensively by in-house guidelines and sanctions for non- compliance are present. Certain large organizations in the private sector may have such guidelines too, but this is not as widespread as one would have liked.

66. The converse option, that is, the regulation of the private sector alone may also present difficulties. It has been debated in other countries before, e.g., Canada, where it was found that the private sector objected to the proposals because it did not see why legislation should cover only private-sector databases. The threat to individual privacy is perceived to be greater in the public sector.

67. The remaining option: legislate for both sectors is probably the preferred option. It is possible however to distinguish between the legislation and its implementation. Thus, it may be preferable to adopt a cautious approach to data protection implementing trial codes of practice on selected sectors like the Direct Marketing sector or the public sector before the full operation of the legislation is effected.

*DATA PROTECTION FOR AUTOMATED DATABASES ONLY?*

68. The Sub-Committee next considered whether regulations should be limited to personal data about natural persons and which is kept in automated databases or whether the law ought to be more extensive.

69. For reasons already explained in paragraph 16 above, the Sub-Committee does not view it appropriate to include non-natural persons into the data protection legislation. The danger is that the legislation may become an instrument to be used for the gathering of business intelligence. Such a occurrence would certainly not be welcome. It ought to be enough to ensure that data about natural data subjects be protected.

*PRIMARY AND SECONDARY LEGISLATION*

70. The Sub-Committee discussed techniques for legislation if such legislation is regarded as desirable. Several options may be considered:

**(a) Omnibus legislation containing rules and principles for all sectors, including sectorial rules where necessary;**

**(b) Main legislation on broad principles and institutions sectorial guidelines (secondary legislation) to be incorporated by reference;**

**(c) Separate main legislation for each sector.**

71. Experience from overseas suggest that Option (a) ought to be eschewed. Such extensive legislation is hard to draft, create enormous problems for implementation, and in an area where changes to technology are so rapid, may become outdated quickly. In 1989, the Committee of Experts on Data Protection set up by the European Committee on Legal Co-operation reported that new technologies are already straining existing Guidelines on which most European legislation are based. The three new technologies said to pose such problems are telemetry, interactive media and electronic mail. All these new technologies are available in Singapore in some form or another. Telemetry - defined as the remote collection of personal data by automatic means - involves such activities as identification of car licence plates, monitoring of use of public utilities or television and so on.

72. An example of interactive media[43] would be the proposed Teleview or videotex services. The banks have also offered such services to their customers. Such services raise data protection problems because everytime a user initiates one of these services, say, by buying an item, or watching a film or transferring a sum of money, he is in a sense providing personal data about his activities, data which may be of great commercial value not only to the service provider but also to other data users.

73. Finally, electronic mail systems may also pose new problems because users of such systems will be communicating more often than not in a confidential capacity and the need for protection with respect to electronic mail becomes obvious.

74. Quite apart from having legislation which can take into account new technological developments, another reason for having broad-based parent legislation supported by sectorial secondary legislation is that there is no need to impose the same obligations on every sector. Some sectors may need to have stricter duties while other sectors can be left very much on their own. We examine this issue in the following paragraphs.

75. Enough has been said to support the view that parent legislation should be broad-based. In the main the primary statute should only state general principles and set up the necessary institutions. The nitty-gritty guidelines ought to be contained in secondary legislation which may be altered with the minimum of difficulty.

*MECHANISMS OF CONTROL*

76. Given that data protection may be prohibitively expensive if undertaken on a grand scale, the Sub-Committee considered whether there should only be selective registration of (or notification by) data users based on the sensitivity of the personal data stored by them. An effort should be made to ascertain what types of data may be regarded as "sensitive" to the general public. Protection may be enhanced where such data is either regarded as sensitive or where the consequences of misuse are great. Records on employment, financial status, medical treatment are examples which would undoubtedly be treated as "sensitive". Grave consequences may also follow from misuse. In the case of medical information, misuse of it may even be life-threatening. On the other hand, data held by individuals for recreation or personal domestic purposes should be totally exempted from any form of control.

77. With respect to sensitive data which needs special protection, the Sub-Committee considered several schemes of control: licensing, registration, notification. There may only be differences of degree among these schemes. Licensing is seen as

an all-encompassing process where all data users have to be licensed by a central authority and where unlicenced users probably would face criminal sanctions. Registration may also have this feature in which case there is no distinction between the two. Most European data protection laws have some form of licensing or registration. The main problem with full-scale licensing or registration is that it requires massive manpower and time to administer and maintain. This may be inversely proportionate to the number of incidents of data abuse and may be unnecessary. On the other hand, a notification procedure whereby data users simply send in minimal information about their operations may be too lax to be effective. It is therefore felt that a combination of control schemes be adopted registration for data users dealing with sensitive data and notification for the rest.

78. A notification-cum-registration scheme will need to distinguish between data users who normally handle sensitive information and those who do not. As mentioned earlier on, what constitutes "sensitive information" needs to be defined. One may follow what the international guidelines have to say.[44] However, that may not be sufficient. The data protection authority should have the discretion and power to stipulate what constitutes sensitive data for the purposes of data protection registration.

79. This option of having a notification-cum-registration should cut down the administrative costs of a data protection agency. The work should be reduced further by the total exemption from the legislation of manual records and personal domestic or recreational records.

80. In terms of sectorial analysis, Singapore may borrow from the experience of other countries in determining where special attention should be paid. For example, in the United Kingdom, special codes of conduct have been drawn up for certain sectors. These include:–

**Education**: school records, records of students in universities and polytechnics;

**Health**: personal health information (including dental or mental health) kept in hospitals or other medical institutions;

**Advertising and Direct Marketing;**

**Employees' data:** such data kept by companies or other governmental institutions.

*DATA PROTECTION INSTITUTIONS*

81. If there should be a data protection agency, it has to be set up with the following functions and consequential powers:

- to implement the legislative principles through their application to sectorial codes of conduct;
- to supervise and maintain a "register" of data-users and to enforce the statutory duties imposed on them;
- to provide data subjects with the necessary information, advice and avenues for complaint and to investigate such complaints;
- to enforce the rights of data subjects.

82. The search for a proper institution to operate as a data protection agency was difficult. Several options were mooted:

**(1) the Attorney-General's Chambers;**

**(2) an appropriate government ministry or department;**

**(3) the National Computer Board;**

**(4) an autonomous institution.**

83. Of these options, Western countries have almost all accepted the fourth option as the obvious choice. There must be no danger of a conflict of interest arising between the data protection agency and the data user. This cannot be guaranteed if it is linked in any way to the data user.

84. The "totally autonomous" approach however is not universal. For example, it is not followed in Japan. Indeed in Japan, the data protection functions are under a unit in the Prime Minister's Office. This may be rationalised on the ground that the data protection legislation covers only the public sector and that the Executive is accountable to Parliament in any event. The Sub-Committee submits that siting the data protection agency in a government ministry or department is not quite appropriate where the legislation covers both sectors. Any discrepancy between the treatment of the two sectors may lead to accusations of unfairness and discrimination. This may be especially so where the alleged offender is a government department or a related statutory agency.

85. Yet, given the acceptance of regulation and guidance from government departments, it may still be a viable option provided that the data protection officials exercise their duties fairly and impartially. The data protection agency could come

under one of the relevant Ministries like the Ministry of Law or the Ministry of Information & Arts.

86. In Singapore, it is felt that the setting up of a special autonomous agency would also be unnecessary given the relatively small size of the database industry and the existence of reasonably independent statutory institutions. The Attorney-General's Chambers, by reason of its constitutional position, may indeed be a viable choice for siting the data protection agency. However, there is also another appropriate statutory body, namely the National Computer Board.

87. The National Computer Board is set up by statute as the main institution responsible for co-ordinating national efforts relating to information technology. Although it is technically under the Ministry of Finance, it operates very much on its own and is under a duty to promote the acceptance of and use of information technology in Singapore.[45] The National Computer Board attempts to make macroscopic policies for information technology in Singapore. It may thus be in a good position to perform data protection functions as it already provides technological guidance to both public and private sectors.

88. This view may however be subject to the Board's own perception of its role: if it limits it to providing only technical know-how and not to enter at all into this area of regulation, then it may not be suitable. At the moment, it does not appear to have the necessary expertise to carry out regulatory functions since its officers are recruited in the main for technological purposes. The Board will certainly need to recruit other types of officers such as legal officers for it to perform regulatory duties effectively.

89. Even if the NCB is suitable, the enforcement of data protection laws require that the agency charged with the duties be invested with sufficiently strong statutory powers of entry, search and seizure. Without such powers, the agency may not be able to carry out its duties effectively. There may also be a need for powers of prosecution to be conferred. This enforcement aspect may be beyond the capabilities of the NCB as it is currently set up.

90. Whether the NCB or another statutory body is given the task to maintain a regulatory framework, it is necessary that a Data Protection Appeals body should be set up to hear appeals from decisions of the data protection agency. Both data subjects and data users should be able to appeal against adverse decisions. The constitution of such a body should include judicial and legal officers as well as information technology professionals from all sectors.

*DATA SHARING*

91. The Sub-Committee has already mentioned data-sharing above. The adverse attitude to data-sharing may not be as pronounced in Singapore as in Europe. For example, even an issue like having national identity cards may draw very negative reactions such as that demonstrated by the UK Data Protection Registrar. In a recent paper on National Identification Systems, the Registrar listed the very real benefits of such systems but at the same time, noted the privacy concerns affected. These include the usual factors about wide replication of errors, using information out of context, using such information for surveillance purposes and so on. The Registrar then concludes that from a privacy and data protection viewpoint, "*the arguments suggest that the step [of having national identity cards] should not be taken.*"[46] Singaporeans do not have such antagonism towards identity cards. It is probable therefore that there will also not be much opposition to data-sharing even in the public sector.[47]

92. Even so, the Sub-Committee feels that data-sharing ought to be controlled by rules which balance the interests of convenience and efficiency against the principles of individual privacy. In particular, the principle that the data subject should have knowledge of, and consent to, data-sharing is vital. Such a principle should be applied to any information which is collected in confidence and for designated purposes, e.g., to apply for a licence or to obtain a loan from a financial institution.

93. Moreover, the principle should also apply wherever information of a sensitive nature is collected or processed even though the data subjects may not have consciously given the information in response to a request. An example of this would be where data subjects use their credit cards to buy goods or services. The usage provides the data users the credit card companies with useful information which was not consciously intended by the data subjects to be conveyed to the data users for any purpose other than obtaining credit on those cards.

94. The Sub-Committee's view is that consent of data subjects must be obtained where the data user proposes to use confidential or sensitive information in a way not intended by the data subject or not contemplated at the time the information is originally collected. Existing prohibitions on data-sharing, especially in the public sector should be institutionalised and procedures streamlined to minimize inconvenience both to data users and data subjects. It has mentioned the principle that data-sharing may be permitted subject to conditions protecting the data from being used in circumstances

where the interests of the data subjects are prejudiced. In all sectors, data-sharing should only be allowed either by specific laws or approved guidelines.

95. The Sub-Committee wishes to emphasize that it perceives the greatest danger to data subjects to be in the sharing of data which may be entered for one purpose and used for another. Erroneous or inaccurate data may cause serious harm to the affected data subjects. Besides this, wrong information also erodes the integrity and usefulness of automated information systems.

96. The Sub-Committee paid special attention to this issue because in certain respects, it is seen as a departure from accepted principles of data protection. The sharing of information among data-bases without cross-matching data is unobjectionable provided it satisfies the data protection principles. It is when the data is not only shared but actually processed to provide more composite details of the data subjects that objections arise. Certain countries have introduced specific legislation to control the cross-matching of personal information by computers.[48] The Sub-Committee therefore believes that data-sharing can be acceptable but cross-matching should be done only under clear guidelines to prevent misuse in both sectors.

*RIGHTS OF DATA SUBJECTS*

97. The Sub-Committee has suggested that the existing rights of data subjects be supported by the creation of additional rights relating to access and amendment or deletion of data held about them by data users. The *raison d'être* for data protection laws is the provision of rights to data subjects. The rights to be conferred in addition to the existing legal rights are stated in the Individual Participation Principle (discussed in para 32 above). Frequently the rights of access and amendment or deletion are buttressed by either criminal sanctions, de-registration or damages against the defaulting data users. Certain interests may however outweigh data subjects' rights.

98. In addition, the Sub-Committee proffers the view that where it is not possible for an self-contained institution to be set up, an aggrieved data subject should be allowed by law to initiate, if necessary, civil and criminal proceedings against a data user who is in breach of statutory rules or codes of conduct. These additional rights are premised on the fact that individual data subjects will guard their interests keenly and where they feel that the appointed agency is not protecting their interests, they ought to have recourse to the courts. They already have certain rights at common-law based on breach of confidence but these additional statutory rights will ensure a reasonable compromise between having to set up a totally autonomous data protection institution

and having one which may be viewed as being under government control. Data users, be they in the public or private sector, will be more cautious about breaching data protection rules. They cannot proceed on the basis that the data protection agency is not likely to take action against them. A data subject, perhaps, could be given a statutory right to damages or injunction against data users who are in breach of (or about to breach) their obligations under the data protection laws.

*EXEMPTIONS*

99. The Sub-Committee acknowledges, as does overseas legislation, that a right of access to data may be subject to other interests. Thus, there can be no right of access to data which are kept for:–

–the prevention or detection of crime;

–national security purposes;

–foreign relations purposes.

Further, there should be no duty to disclose information which may affect national economic interests or which is not at present allowed under other laws.

100. All national legislation on data protection accept that there must be exceptions to the obligations of disclosure. The interests of data subjects may be overridden by those interests affecting national security or public safety. Thus, a suspect should not be allowed to gain access to information about an on-going investigation into his alleged criminal activities. To allow this may hamper the administration of justice to an unacceptable degree. *A fortiori*, where data concerning foreign relations or economic interests are concerned, there should be no duty to register or disclose such data. The present restrictions on disclosure for privileged documents, for example, must also be noted.

END OF PAPER

*(Footnotes on next page)*

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

FOOTNOTES

[1] The members are: Assoc Prof Chin TY (NUS, Chairman), Mr Jeffrey Chan (A-G Chambers), Mr David Hew (Advocate & Solicitor), Mr Tan Chee Meng (A-G Chambers, Secretary), Mr Lee Kwok Cheong (NCB).

[2] The National Computer Board in its Yearbook 1988/9 documents an astonishing growth in the use of computers in all sectors. In the public sector, the Civil Service Computerisation Programme (CSCP) is in full swing: examples of ancillary programmes either planned or in effect are ID Net, Data Adminstration Programme, Teleview. In the private sector, TRADENET (which of course also involves public sector departments), MediNet, SECP are all examples of an ever- growing wave of computerization. Introduction of electronic road pricing may also affect the privacy of individuals as their journeys are monitored.

[3] Law Reform Commission Report 22, Vols 1-3 (1983), hereinafter referred to as ALRC 22.

[4] ALRC 22, Vol 1, para 118.

[5] However, some Eastern European countries, e.g., Hungary, already have drafts of data protection legislation.

[6] The most influential international instrument is the Council of Europe Convention, Treaty 108 which is based on the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, effective 23 Sept 1980.

[7] For instance, persons surveyed on what they eat may give more casual answers which may be unsuitable for health insurance purposes.

[8] See Art 12, Council of Europe Convention, Treaty 108, 1981.

[9] Unlike the established professions accountants, doctors, engineers, and lawyers, it is not easy to decide what types of computer personnel should be subject to professional rules of conduct. However, it may be better to approach the subject not from the personnel perspective but from the nature of the information kept.

[10] UK Report of the Committee on Data Protection, 1978, HMSO Cmnd 7341, p xix.

[11] The *Data Protection Act 1984 (UK)* defines data as information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose: s 1(2) The Irish legislation defines data more broadly as information in a form in which it can be processed (*Data Protection Act 1988 Ireland*)

12 The Australian *Privacy Act 1988* (No. 119) is an example of a fairly wide piece of legislation. Even so, it is limited to personal information as defined in s 6(1).

13 See, Patrick Birkinshaw, **Freedom of Information**, 1988 (Wiedenfield & Nicholson). The information need not be about the individual seeking disclosure. It may be on a matter of public interest, e.g., decisions made to build schools etc.

14 Australia has a Freedom of Information Act and a Privacy Act.

15 See Gavison, *Privacy & the Limits of Law*, (1980) 89 Yale LJ 421.

16 This definition is interesting: (a) it does not apply to legal persons and (b) it does not require that the information be given by the individual. It may be the result of surveillance.

17 See also, the definition in the US Privacy Act 1974 which includes voice-prints and photographs.

18 This term refers to any person, including corporate persons, who uses personal information.

19 It is not intended here to review the law in its fullest detail. Such an exercise may add substantially to the length of the report. Excellent legal works, particularly on the common-law remedies are plentiful. Only an outline of the problems under existing law will be given.

20 All references to Singapore statutes are based on the 1985 edition unless otherwise stated.

21 See section 5(1)(iv), Official Secrets Act, Cap 213.

22 Section 47. Subsection (4) provides for authorised disclosures. The phrase relevant particulars is wide enough to cover personal details of customers, e.g., his credit status, assets, debts and so on.

23 Colin Tapper, **Computer Law**, 4 ed. (1989) Longmans, p 359.

24 See also, Legal & Constitutional Committee, 40th. Report to Parliament (Victoria), *Privacy & Breach of Confidence* (May 1990).

25 See Evidence Act, sections 123-128.

26 Annex to Recommendation of the Council, Sept 23, 1980, OECD Paris 1981.

27 The full title is Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data. The Treaty was open for signatures on 28 Jan 1981.The Explanatory Notes to the Convention (at para 24) stressed

[46] Data Protection Registrar Paper dated February 2, 1989. See also Press Release of 9, Feb 1989 suggesting "voluntary" identity cards.

[47] It is worth noting that TIME magazine reported in 6 July 1987 that by means of a computer-matching technique, removing the names of dead persons from the Social Security files saved the authorities US$50 million.

[48] Computer Matching and Privacy Protection Act 1988 (US) amending the Privacy Act 1974.