TOWARDS A PERSONAL DATA PROTECTION REGIME IN MALAYSIA

Background

Data protection is a relatively new legal concept.[1] Within the context of privacy, it is often referred to as 'information privacy',[2] that is, the interest of the person in controlling the information held by others about him. The first data protection law is said to have been enacted in the German state of Hesse in 1970 although Sweden was probably the first country to enact a national data protection law in 1973.[3] International initiatives on rules and guidelines governing data protection soon followed suit and in the 1980s, the Organisation for Economic Cooperation and Development (OECD) released its Guidelines Governing the Protection of Transborder Data Flows of Personal Data,[4] and the Council of Europe, the Convention for the Protection of Indi-

[1] This emerging area of the law is referred to as 'data protection' in Europe, while in countries such as the United States of America, Canada and Australia, the term typically used is 'privacy protection'.

[2] The other aspects of privacy include 'territorial privacy', that is, interest in controlling entry to the personal place; 'personal privacy', that is, the interest in freedom from interference with one's person; and communications and surveillance privacy, the interest in freedom from surveillance and the interception of one's communications. Although there is a link between data protection and privacy, the former is not concerned with the preservation of privacy as such but with the use to which personal data, which may or may not be private information, could be put.

[3] Lloyd I J *Information Technology Law* 3rd Ed, (London, Butterwoths, 2000) at para 4.3; Global Internet Liberty Campaign, *Privacy and Human Rights – An International Survey of Privacy Laws and Developments* 8, 10 October 1998.

[4] The Guidelines were adopted on 23 September 1980 followed by the 1985 Declaration on Transborder Data Flows and the 1998 Ministerial Declaration on the Protection of Privacy on Global Networks.

viduals with regard to the Automatic Processing of Personal Data.[5] These two initiatives are considered the precursors of current data protection laws, and together with the EU Data Protection Directive (95/46/EC), provide useful basic principles for data protection.

The Malaysian Government is in the process of formulating a draft data protection law, the aim of which is to regulate the collection, holding, processing and using of any data or information pertaining to an individual person, such as name, date of birth, address, sex, finances, preferences, etc. This idea of a data protection law was mooted as part of the Government's effort to create a legal and regulatory framework for the Multimedia Super Corridor or MSC project.[6] Towards this end, the Government enacted in 1997, what is now collectively known as the 'Malaysian Cyberlaws' comprising the Digital Signature Act, the Computer Crimes Act, the Telemedicine Act and amendments to the Copyright Act 1987. At that time, it was envisaged that, where necessary, laws would be enacted for matters such as the protection of consumers in relation to transactions over the network environment, the convergence of technologies as well as the collection, storage, retrieval and dissemination of personal data. In so far as the convergence of technologies was concerned, the Communications and Multimedia Act was enacted in 1988 to deal on a single platform the regulation of telecommunications, broadcasting and electronic networks.[7] Work on the personal data protection law commenced thereafter but it was not until November 2000, that the Government, in an unprecedented move, released a draft version of a proposed bill for the protection of personal data for public comment (hereinafter referred to as the 'Proposed Bill').

Potentially, the Proposed Bill, if and when enacted, would cover practically any person or body that collects any information relating to persons such as employees, customers, clients, members of organiza-

[5] The Convention was signed in Strasbourg on 28 January 1981 and came into effect on 1st October 1985.

[6] For further information on the project, see http://www.mdc.com.my (last accessed 21 November 2003).

[7] Originally, the proposal was to include provisions for the protection of data under what was then known as the Multimedia Convergence Bill. However because of the breadth and scope of the subject matter of convergence as well as of data protection, the decision was to enact separate laws for these two areas.

tions or societies, patients, citizens, suppliers, business associates or even friends. The proposed law will entail fundamental changes to current policies and practices relating to the collection, holding, processing, use and disclosure of personal data; such policies and practices will have to be re-examined, and new ones will have to be put in place to ensure compliance. Our personal perception of the value and potential abuse of data relating to us will also have to change.

By reason of its potential implications and its relative novelty in Malaysia, and indeed in most parts of the world, the proposal to enact a personal data protection law has raised and continues to raise various concerns. First, there is the issue of whether the proposed law should also apply to the government, including state and local governments, and statutory bodies, or should be restricted to the private sector only. Paramount in the evaluation of this question is the implication of excluding the government and the public sector. The government, through its various registration, tax and other agencies, is one of the largest collectors and custodians of personal data in the country. As such, to exclude it from the ambit of a personal data law would be to deny the underlying objectives of such a law. On the assumption that such law applies equally to both the public and private sectors, the next issue is the status of the supervisory body responsible for the enforcement of the law. Is such body to be a government entity, to be placed under the jurisdiction of a particular Ministry or agency, or should it be independent of the government, answerable perhaps only to Parliament? The third issue relates to the relationship between the proposed law and other existing laws and the resolution of any inconsistencies that may arise. In such a situation, should the proposed law prevail over the existing laws, subject only to any exemptions that may be provided in the former, or should the proposed law have only prospective effect, with the existing law continuing to apply even with inconsistencies? Fourthly, what are the exemptions that would be provided in order that matters relating to national security, public policy, crimes and health records are not affected by the need to comply with data protection principles? Fifthly, given that this is a new law, processes, education, change management and procedures will have to be put in place to ensure compliance with it, which in all likelihood will involve considerable costs, time and resource. In normal circumstances, and more so in the current economic situation, the tough question facing the govern-

ment is whether the benefits of the proposed law outweigh the costs of implementing it so as to justify its enactment. Sixthly, there may be undue restrictions on flow of information necessary for purposes of promotion, planning, marketing, as well as research and development work in new technologies and other areas. This includes the restriction on transborder flow of data to countries that are not specified by the Minister or which do not offer the same level or adequate level of protection to personal data. Last but not least, the costs and procedures associated with compliance may have the undesirable effect of lessening the competitive advantage of this country, thereby affecting the inflow of investment.

As a result of the above concerns, the Malaysian Government did not table the Proposed Bill in Parliament in mid-2001, as originally intended. Instead, the Government commissioned a study to examine the above and other issues and to make recommendations on how to deal with the possible implications and effects of the proposed law. Presumably, the whole rationale underlying the need for such a law would also be examined. It is likely that the study would result in changes to the Proposed Bill. However, it is unlikely that there would be substantial changes to some of the basic principles of data protection as provided in the Proposed Bill, most if not all of which were based on international practices. On this basis, this short note will examine some of the salient features of the Proposed Bill.

Rationale for the Protection of Personal Data

Basically, the aims of the Proposed Bill are to regulate the collection, possession, processing and use of personal data by any person or organisation so as to provide protection to an individual's personal data and safeguard the privacy of an individual; and to establish a set of common rules and guidelines on the handling and treatment of personal data by any person or organisation such that these rules and guidelines will form the basis for the protection of personal data and at the same time ensure free flow of information.[5] The objectives underlying the proposed law are to provide adequate security and pri-

[5] As stated in the website of the Ministry of Energy, Communications and Multimedia: see http//www.ktkm.gov.my (last accessed 21 November 2003).

vacy in handling personal information; create confidence among consumers and users of both networked and non-networked environment; accelerate uptake of electronic transactions; and promote a secure electronic environment in line with the objectives of the MSC.[9]

From the above, three main reasons may be cited as the driving forces for the legislation of a personal data protection law in Malaysia. It is believed that these reasons will continue to be relevant notwithstanding any other recommendations by the Government's consultant.

First, the ability of technology to gather, store, retrieve, correlate, disseminate and manipulate personal data has given rise to concerns that the privacy of the individuals may be disregarded or abused, if it is not already. While it is accepted that digital processing technology would allow the use, disclosure or dissemination of information collected without the knowledge or consent of the data subject, and making it possible to form opinions, make judgements, identify habits and even create by way of data matching a detailed profile of an individual's lifestyle, tastes, political views and health, there are also fears of manipulation of data or use or storage of outdated, incorrect or misleading information. It is noteworthy that concerns over the ability and implications of computers to store, link, manipulate and provide access to information were already expressed as far back as the early 1970s.[10] When extrapolated against a background of global computer networks and transborder data flow, and the lack of adequate legislation regulating the protection of personal data, the gravity and enormity of these issues increase manifold. Although the collection and use of personal information has been going on from time immemorial, the traditional method of collection and filing in cabinets or their equivalent are not quite the same as what newer technologies can do in terms of enabling data to be retrieved, disseminated and matched. These concerns formed the thrust behind the proposal for the protection of personal data when it was made in a report prepared for the Malaysian National Informa-

[9] *Ibid.*

[10] See, for instance, the *UK Report of the Committee on Privacy* Cmnd 5012, London HMSO 1972, (Younger Report) which identified amongst others, the areas of concern as follows: the computer's ability to compile information; the ability to provide access; and its power to correlate information: para 581. The Report also provided 10 guidelines for the collection, handling, access and use of computerised records: paras 592-600.

tion Technology Council or NITC in 1996 entitled *Laws and Policies Affecting the Development of Information Technology*.[11] In that report, it was envisaged that with the increasing use of computers, and the ability of digital processing technology to collect, process, store, retrieve and disseminate voluminous amount of data, the public and private sectors would eventually replace their manual filing systems with computerised storage systems. While accepting the benefits that technology would create for data collection, processing and storage, it was also mindful of the impact that such activities, which would take place both domestically and internationally, would have on the privacy of the individual. Accordingly, the report recommended that a data protection law be enacted, not only to protect the privacy of the individuals and to ensure that data subjects have some form of control over the use of personal information collected about them, but also to ensure the free flow of information and the growth of the data processing industry.

Much has happened since the report. Developments in information and communication technologies have increased the capacity to collect and distribute personal information, which may pertain to details such as name, age, religion, physical characteristics (like finger prints, voice recognition, retina) and preferences etc, and store such information in electronic data banks, smart identity cards and biometrics and genetic databases. If in the past, personal information was collected with the co-operation, real or otherwise, of the data subjects, in the sense that it was provided by or with the consent of the data subjects themselves, currently a variety of tracking, surveillance, copy-protection technologies,[12] file-sharing and spyware software and

[11] The report, of which the writer was part, was prepared prior to the launching of the MSC. Later, it was used as one of the reference materials for the formulation of the legislative and regulatory framework for the MSC.

[12] Copy-protection technologies and digital rights management systems are being developed for use by copyright owners to regulate access to copyright material and for purpose of rights management. While the use of such technologies has been legally recognized, (see the Copyright Act 1987, s 36(3) and (4) it has also raised concerns that such technologies may enable customer profiling and prevent anonymous usage of content: see further, Greenleaf G., "IP, Phone Home: The Uneasy Relationship between Copyright and Privacy Illustrated in the Laws of Hong Kong and Australia" (2002) 32 HKLJ 35.

communication technologies[13] exist which permit the gathering of personal information without any actual input by or knowledge of the data subjects. Browsers are one such tool of surveillance. A user when using a browser to access a website, faces the possibility of information such as his email address, the type of computer, the hardware or software being used, the links clicked on or websites accessed, being transmitted and stored on servers. Browsers may also support cookies[14] which are unique identifiers that web servers placed on computers and which typically are strings of long-random looking letters, used to track the user's movements on web sites. The information gathered could be exchanged or combined and subsequently used for advertising or other content-related purposes.[15]

The use of tracking and surveillance technologies to counter the threat of terrorism and to collect information relating to such activities has also increased, particularly after the events of September 11, 2001, and this usage will pose even greater challenges to the informational privacy of the individuals. As Lord Hoffmann very aptly put it in *Reg v Brown (Gregory)*,[16]

> .....one of the less welcome consequences of the information technology revolution is the ease with which it has become possible to invade the privacy of the individual. .... Vast amounts of information about everyone are stored on computers, capable of instant trans-

[13] An example is electronic numbering (ENUM) which is a protocol for translating telephone numbers in Internet Domain Names and mapping telephone numbers to other means of communication such as email, fax and mobile numbers. It creates an unique identifier and allows personal information about individuals who have ENUM to be made publicly accessible in a database on the Internet.

[14] Netscape defines cookies as 'a general mechanism which server side connections (such as CGI script) can use to both store and retrieve information on the client side of the connection'. It is a mechanism that allows a web site to record the online user's activities over the Internet, usually without the user's knowledge or consent.

[15] For example, DoubleClick Inc., an Internet advertising firm, allegedly used cookies to track the online activities of Internet users. When it announced its intentions of combining the information it had collected with the database of a catalogue database firm, with which it had merged, a complaint was filed against it in the US Federal Trade Commission on 10 February, 2000.

[16] [1996] 1 AC 543 at 556.

> mission anywhere in the world and accessible at the touch of a keyboard. The right to keep oneself to oneself, to tell other people that certain things are none of their business, is under technological threat.

Hence, it is even more imperative than ever that those developments in technologies that allow and facilitate the collection, analysis and dissemination of data about individuals do not encroach upon the privacy of an individual.

Secondly, electronic commerce and transactions, both in the public as well as the private sectors, have also taken off or are in the process of taking off in various parts of the world. The success of electronic commerce is dependent on a number of factors, such as the availability of the necessary infrastructural support, the existence of a legal and regulatory framework and the acceptance of this mode of transaction, but security and privacy are often cited as the main reasons for the slow uptake of electronic transactions. Consumers are generally concerned about the security of their financial details, be it when transmitted over the network to the relevant parties or when stored in the servers of the said parties. Of equal concern is the use to which such details as well as other non-financial and personal information may be put, thereby infringing their privacy. These concerns over tampering and use of personal and financial information need to be addressed in order that a conducive environment for electronic commerce may be built. As the Proposed Bill explains,

> New technologies, increasing data collections, changing market trends and the new global market place for electronic commerce are contributing to the increasingly important role of information in the global economy. As such, information particularly has become a valuable commodity that can bring jobs, business and customer services. Hence, these factors have increased mounting pressure to collect, hold, process and use personal data more than before. These factors have also reduced the level of privacy and consumer confidence is lacking in such environment.

While the concern over personal data privacy may be met by measures taken by the relevant merchants or service providers, such measures are merely voluntary and therefore may not provide the necessary

reassurance so vitally needed in the global market place.[17] The uneven self-regulatory landscape may need to be supplemented by a statutory scheme under which the minimum requirements for protecting personal data are made mandatory.

Thirdly, there is also a need to respond to international and legislative developments elsewhere, which have seen the formulation of various guidelines on privacy and data protection and the enactment of data protection or privacy laws. The driving forces behind this development, however, were not the challenges posed by technology in information collection, storage, use and dissemination. According to Bygrave, data protection laws owe their origins to 'a complex array of factors' such as ideological, organizational, and economic, and computers are just one other important element.[18] Bygrave cites, among others, the growth in the 1960s and 1970s in the amount of data collected by various types of organisations, the integration of these data into centralised data banks, the sharing of personal data by agencies, and the modern organisations appetite for information as factors that triggered off concerns for the protection of privacy. The reasons underlying such development thus predated the onset of the computer age although the increasing use of automation has added to the growing concern.

Ideologically, the protection of personal information is perceived as a fundamental right against the encroachment of an individual's privacy as reflected in Article 12 of the Universal Declaration of Human

---

[17] It is interesting to note that in the US, where there is no general law regulating data collection, most web sites, including almost all the top 100 web sites, other than those specifically required to do, such as those directed to children or other regulated sectors, do post, as a matter of good commercial practices, privacy statements on their own accord. Any violation of such statements may constitute 'unfair or deceptive acts or practices or affecting commerce' within the meaning of s 5 (a) of the Federal Trade Commission Act (15 USC s 45(a) (1)) and expose the website providers to criminal liability: see further, www.ftc.gov/ogc/brforvw.htm.(last accessed 21 November 2003). According to a survey conducted by Manches and reported by the Financial Times dated 3 April, 2001, 44% of e-traders complied with data protection 4% of 300 businesses sought any legal advice when setting up web sites and 44% had no policy on staff' use of email or Internet.

[18] See Bygrave L *Data Protection Law- Approaching Its Rationale, Logic and Limits* (Kluwer Law International, 2002), at 377. See too at 93-95.

Rights which specifically protects territorial and communications privacy in the following terms:

> No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks.[19]

Both the OECD's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data and the Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data[20] were formulated in recognition of the fundamental principle that the privacy and individual liberties should be protected. In the 1990s, the European Union, on the basis that the free movement of goods, services and capital from one member state to another also entails the free movement of data, and that such movement should be balanced against the right to privacy, enacted the Data Protection Directive (95/46/EC) and The Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (Directive 97/66/EC 15 December 1997).[21]

The EU Data Protection Directive (95/46/EC), which has as its main objectives, the protection of personal information about individuals and the prevention of any restrictions on the free flow of personal information between member states, sets the benchmark for the national law of each member state which will harmonise the law on data

---

[19] It is interesting to note that under the Charter of Fundamental Rights of the European Union 2000, data protection was recognized as a autonomous, fundamental right of individuals to be kept separate from the broader right with respect to private and family life: Arts 8 and 7.

[20] The UK Data Protection Act 1984 was enacted to enable the United Kingdom to ratify the said Convention: see *Reg v Brown (Gregory)* supra n 16 at 557 (Lord Hoffmann). See too Jay R & Hamilton A *Data Protection Law & Practice* (London, Sweet & Maxwell, 1999) at paras 1-16-1-19.

[21] This Directive imposes obligations on telecommunications carriers and service providers in relation to communications by users and personal details.

protection throughout the EU.[22] It establishes various principles upon which data collection, use and access may proceed. It also requires member states to ensure that transfers of any personal information relating to European citizens are permitted only to countries outside the EU where there is adequate protection for such data, unless one of the exceptions applies.[23] Once an EU member has decided to block a transfer on the basis of inadequacy, this decision will apply to all other members.[24] To assess the adequacy of the level of protection afforded by a third country, consideration would be given to the nature of the data, the purpose and duration of the proposed operation, the country of origin and the country of final destination, the rules of law in force in the country in question, and the professional rules and security measures which have to be complied with in that country.[25] A country with no protection or no adequate protection for personal data may thus face hindrances in the flow of information from EU member states a situation which will definitely have considerable impact in this age of globalised trade and commerce.

That Malaysia may face possible trade barriers on account of its lack of protection for personal data, was one of the reasons that prompted the Government to consider the legislation of a data protection law framed in terms adequate to meet the requirements of the EU Directive.

---

[22] The EU Data Protection Directive entered into force on 24 October 1998 and as of September 2002, has been implemented into national law by all member states except Ireland and Luxembourg: see http://europa.eu.int/comm/internal_market/en/dataprot/law/impl.htm (last accessed 21 November 2003).

[23] Art. 25 of the EU Data Protection Directive. The European Working Party established under Art 29 has the power to give to the Commission an opinion on the level of protection in third countries. See too Art 31(2) of the Directive. On 26 July 2000, the Commission decided that the US' Safe Harbor Privacy Principles issued by the US Department of Commerce provided an adequate level of protection for personal data transferred from member states to the US. A similar decision was made with respect to the Canadian Personal Information and Electronic Documents Act 2001 on 14 February 2002.

[24] See, for instance, the UK Data Protection Act 1998, Sch 1, Part II, para 15.

[25] Art 26(2) of the EU Data Protection Directive.

Models for the Protection of Personal Data

Privacy laws aside, there are various ways by which protection of personal data may be achieved. One method is by way of comprehensive legislation or regulation. The legislative or regulatory model can be further subdivided into three approaches. One approach takes the form of a law of general application, which imposes data protection restrictions on both the government and the private sector. Examples of countries which have adopted this approach are Hong Kong[26] and the United Kingdom.[27] The second regulatory approach favours specific sectoral laws to regulate the handling, use and dissemination of information or data. Under this approach, different laws could apply to the government and the private sector, as in the case of Australia[28] and Canada,[29] or within the private sector, specific provisions could be made to apply to various segments such as the financial services industry, consumers, etc., as in the case of the United States.[30] The third approach is a mixture of regulation and self-regulation or what is known as co-regulation. Under this approach, the self-regulatory framework is provided and is backed by statutory provisions, thus giving it flexibility to deal with the specific issues of each industry and at the same time the force of law.

The second method that has been adopted is that of self regulation by the industries concerned, typically with relevant codes of practice

---

[26] The Hong Kong Personal Data (Privacy) Ordinance (Cap 486).

[27] The UK Data Protection Act 1984 which was subsequently replaced by the UK Data Protection Act 1998.

[28] Australia has two main federal laws in the form of the Privacy Act 1988, which applies to Commonwealth agencies, and the Privacy Amendment (Private Sector) Act 2000 which applies to organisations in the private sector. The latter has provisions for privacy codes applicable to sectors of industry. See generally Jackson, M, *Hughes on Data Protection in Australia* 2nd Ed (Sydney, Lawbook, 2001).

[29] The Privacy Act of 1983 limits the Federal Government's ability to collect, use or disclose information on Canadians, while the Personal Information Protection and Electronic Documents Act, passed in 1991, applies to the private sector.

[30] See, for instance, the Children's Online Privacy Protection Act of 1998; the Right to Financial Privacy Act of 1978; and the Video Privacy Protection Act 1988.

or conduct, and without any legislative intervention.[31] The third method, which is one that should be adopted regardless of the legal environment, is by individual users themselves using the various privacy enhancing technologies or software available, which may be used to ensure email and file privacy, anonymous surfing, disable cookies, encryption, etc.[32]

The Proposed Bill has adopted the co-regulatory approach but the model may well change after the consultant's study. The Proposed Bill provides for a regulatory structure with a Commissioner for Personal Data Protection playing administrative, supervisory and promotional roles, such as advising the Minister on all matters concerning national policy objectives for data protection activities; monitoring and supervising compliance with the provisions of the Bill; and promoting awareness and understanding of the requirements of the Bill. The Commissioner receives and investigates into any complaints on contravention of the provisions of the proposed law. Where the Commissioner is satisfied that a data user has contravened any of the data protection principles, and that the contravention is a matter that has caused or is likely to cause damage or distress to any individual who is the data subject of the personal data concerned, he may serve on the data user an enforcement notice, directing the data user to take such steps to remedy the contravention. It is an offence not to comply with an enforcement notice.

The Proposed Bill does not require data users to register with or notify the Commissioner as a pre-condition for the collection of personal data; it merely makes it obligatory for the data users to comply with the various statutory provisions as well as with codes for practice as may be applicable to them. However, the Minister may specify that certain classes of data users be required to register with the Commissioner. These data users are required to submit particulars relating to the type of personal data to be collected, held, processed or used, the

[31] See, for instance, the Singapore Model Data Protection Code for the private sector drafted by the National Internet Advisory Committee (NIAC) with input from the information technology, health and media industries, and small and medium enterprises. The Code was launched on 5 February 2002.

[32] For a list of practical privacy tools, see www.epic.org/privacy/tools.htm (last accessed 21 November 2003).

source of the personal data, a description of the person to whom the data user intends to disclose the personal data, etc.[33]

While the proposed law provides guiding principles for the collection and use of personal data, it is envisaged that legislative efforts would be augmented by a self-regulatory framework. The Proposed Bill provides for the designation of a data user forum where the Commissioner is satisfied that the membership is open to 'all relevant data users'. This would appear to suggest that data user forums representing specific industry interests could be formed and provided all the statutory requirements are met, designated as the relevant industry-specific data user forum. The function of this forum is to regulate collection and use of personal data among its members by means of code(s) of practice. The code of practice may be prepared by the data user forum or, if no code is so prepared, by the Commissioner. For the purpose of the Proposed Bill, such code must be registered with the Commissioner, and with the respect to the code prepared by the Commissioner, such registration is automatic. However, with respect to the Code prepared by the data user forum, registration is dependent on whether the code of practice is consistent with the provisions of the Proposed Bill and that in the course of preparing the code, public consultation has been held. Once registered, any failure to comply with any provisions of a code of practice will attract a civil penalty of a fine not exceeding RM 200,000. On the other hand, compliance with the code shall be a defence against any prosecution, action or proceedings of any nature in respect of any matter dealt with in the code.

Salient Features of the Proposed Personal Data Protection Bill

Although its ramifications and effects are far-reaching, it should be emphasised that the Proposed Bill does not attempt to prohibit the collection, holding or processing or use of personal data; nor does it deal with access to any information collected. In other words, the proposed law is not a law relating to privacy, as traditionally understood, or freedom of information. Rather, it requires the person collecting, processing, holding and using personal data collected by him to comply with certain prescribed principles.

[33] Second Schedule to the Proposed Bill.

Scope of the Proposed Bill

'Personal data' is defined as any information recorded in a document in which it can practically be processed wholly or partly by any automatic means or otherwise. Information that is not recorded, that is, in oral form, is excluded. The information must also be capable of being processed, that is the carrying out of any operation or set of operation on personal data and includes recording, amendment, deletion, organization, adaptation, alteration, retrieval, consultation, alignment, combination, blocking, erasure, destruction or dissemination of personal data.[34] However, it is not clear whether the information 'recorded' must have a certain degree of permanence or life span. The fact that it could be processed does not necessarily indicate storage for a certain length of time as processing could take place even if the information is recorded for only a very short time, as may be illustrated by the English case of *Reg v Gold*.[35] In that case, the issue was whether an act of unauthorised access into a computer network by the entry of a number and password constituted making a false instrument under section 1 of the Forgery and Counterfeiting Act 1981. The word 'instrument' is defined under section 8(1) to mean 'any disc, sound track or other device on or in which information is recorded or stored by mechanical, electronic or other means'. In interpreting the meaning of 'recorded or stored', the House of Lords resorted to their ordinary and natural meanings and held that the words connoted the preservation of a thing for an appreciable time with the object of subsequent retrieval or recovery, and as the information comprising the number and password was only stored or recorded momentarily during automatic verification by the system and the cleared, there was no recording or storage as such.

The scope of the Proposed Bill covers information however recorded, whether manually or by automated means. Although this may prove burdensome, the non-discriminatory approach ensures that

[34] As defined in clause 2. Except for some differences, this definition is similar to that under the UK Data Protection Act 1998. For the differences between 'processing' and 'using' see the decision of the House of Lords in *Reg* v *Brown* [1996] *supra* n 16 at 561-562, per Lord Hoffmann.

[35] [1988] 1 AC 1063.

there will be no confusion as to its application particularly in situations where data may be kept in both manual files and computerised form, or in either form.[36]

The information may be contained in a disc, film, tape or other device and includes not only text but visual images such as photographs and films as well. The inclusion of visual images suggests that data is not restricted to information of a textual nature alone and that it includes photographic and other visual images on any form. The overall effect is to provide individuals some form of protection in so far as the recording of their images is concerned. As Wong JA describes it in *Eastwick Publisher Ltd & Anor v Privacy Commissioner for Personal Data*,[37]

> A photograph can tell many things. It tells the race, sex, approximate age, weight and height of the person shown in the photograph. On the other hand, the written description of a person.....does not tell very much about the person.... The person in the photograph can only be the person himself or herself and no one else.[38]

The personal data must be information which identifies the individual or which can be linked to any identifiable individual, for instance, by name, identity card number, account number or photograph. Identification is not restricted to the particular data alone; it is sufficient if the data subject could be identified using or by reference to other information held by the data user. The need for some form of identification, however, may act to limit the scope of the proposed law, as may be illustrated by the Hong Kong case of *Eastwick Publisher Ltd & Anor v Privacy Commissioner for Personal Data*.[39] In that case, a photographer working for the plaintiff and using long-range lenses, took

---

[36] The former UK Data Protection Act 1984 applied only to information recorded in computer-readable form. In *Reg v Brown* supra n 16, Lord Hoffmann observed in passing the paradoxical consequences that could arise because of this restricted application: see 560. The current UK Data Protection Act 1998 makes no such distinction.

[37] [2000] 2 HKLRD 83.

[38] *Ibid* at 99.

[39] *Supra* n 37.

pictures of the various women seen on the streets of Hong Kong. The photographs which were taken without the consent or knowledge of the subject matter, did not identify the women by their full names but by first names in quotation marks or some description phrases, some of which were not flattering. One of the women photographed filed a complaint with the Hong Kong Privacy Commissioner for Personal Data. The Commissioner found that the personal data in the form of the photograph had been collected by unfair means thereby violating the first data protection principle in the Personal Data (Privacy) Ordinance (Cap. 486). Having failed to quash the decision of the Commissioner, the plaintiff appealed to the Court of Appeal. Two main issues were canvassed: first, whether a photograph of a person constituted 'personal data' and secondly, whether the taking of the photograph amounted to a collection of personal data within the Ordinance. While the Court of Appeal was unanimous that a photograph was personal data, there was a split in relation to the second issue. By a majority, the Court of Appeal held that the taking of the photograph in the circumstances of that case did not constitute an act of personal data collection. According to Ribeiro JA,

> It is... of the essence of the required act of personal data collection that the data user must thereby be compiling information about an identified person or about a person whom the data user intends or seeks to identify. The data collected must be an item of personal information attaching to an identified subject, as the ... definitions of 'personal data' and 'data subject' suggest.[40]

Hence, where the complainant was photographed and where the photographer was not concerned about her identity nor needed it for his newspaper article, there was no collection of personal data. Being used as an anonymous subject of a photograph did not amount to a collection of personal data. Wong JA, however, in a minority judgment held that the taking of the photograph amounted to an act of collection and that its collection was unfair in the circumstances of the case.

---

[40] *Supra* n 37 at 90.

Personal data includes any expression of opinion about an individual, and any indication of the intentions of the data user with respect to that individual. This would cover, for instance, evaluation or appraisal reports of an employee.

The scope of protection is limited to personal data of living individuals; it does not include information about a dead individual nor does it cover other persons such as companies or businesses .

The person collecting the data is known as the data user while the subject matter of the data is the data subject. The data subject must be a natural person who is still alive. There are provisions with regard to data subjects who are minors or persons with incapacities. The person who can act on behalf of the minor is the guardian while as far as the latter is concerned, the person who can act is someone appointed by the court.[41] The data user is any person who controls the collection, holding, processing or use of personal data. Such data user may include the Government, non-government organizations, companies, business, institutions and individuals. Although a data user includes companies, the proposed law is silent as to whether companies within the same group are treated as one entity. In so far as the Government is concerned, it is clarified that each government department is to be treated as a government department separate from any other government department.[42]

The definition of 'data user' excludes those who collect, processes, holds or uses data on behalf of someone else, such as an Internet service provider who stores emails or transfers files. The exclusion, however, does not apply if the person on whose behalf that data is being collected is outside Malaysia, in which case the person collecting, processing, holding or using the data is treated as the data user.

Principles of Data Collection

The Proposed Bill gives various rights to the individuals with respect to personal data held by a third party. Basically, it requires any data user to comply with nine prescribed principles when collecting,

[41] See definition of 'relevant person' in clause 2 of the Proposed Bill.

[42] Clause 3(2) of the Proposed Bill.

processing, holding and using personal data as set out in the First Schedule[43] and are as follows:

Data principle 1 relates to the manner of collection which must be fair and lawful. Under this principle, the data user must inform the data subject, among other things, of the purpose of the collection, whether there is an obligation on his part to supply it, and the data subject's right to access and correct the data collected.

Data principle 2 is concerned with the purpose of collection of personal data. Under this principle, personal data shall be held only for one or more specified and lawful purposes. The collection must be related to the function or activity of the data user and must be adequate and not excessive for the purpose.

Data principle 3 deals with the use of personal data and provides that data shall not be used for purposes other than that for which it was collected unless there is consent by the data subject.

Data principle 4 provides that data shall not be disclosed without consent of the data subject unless the disclosure is done for the purpose for which the personal data was collected.

Data principle 5 requires all practicable steps to be taken to ensure that personal data is accurate, complete, relevant, not misleading and up-to-date.

Data principle 6 prescribes that personal data shall not be kept for longer than necessary for the purpose for which it was collected.

Data principle 7 deals with access to and correction of personal data. Under this principle, a data subject is entitled to be informed by the data user of any personal data of which the individual is a subject, and where appropriate to have it corrected.

Under principle 8, all practicable steps shall be taken to ensure security of data. The data user is required to ensure that measures are in place to guard against unauthorized or accidental access, erasure, destruction or disclosure of data.

Data principle 9 provides that a data subject must be able to ascertain data user's policies practices in relation to personal data and the kind of data held by the data user.

The rights of the data subject and the duties and rights of the data user are more specifically provided for under Part IV of the Proposed

[43] Clause 4(1) of the Proposed Bill.

Bill. Generally, the individual or data subject has the right not to have his personal data used or disclosed for purposes other than the purpose in connection with which the personal data was collected, held or processed. Corollary to this right is the right to have personal data erased when it is no longer required for the purpose for which it was held or used in the first place.

Other rights include the right of access to personal data held, which is basically the right to be informed of the personal data held, and where the processing of the data is by automatic means, to be informed of the logic involved in the decision-taking. The data user is statutorily bound to provide the above information upon request in writing from the data subject or a person acting on behalf of the data subject who is a minor or who is not capable of managing his own affairs, or an authorised person. The data user is bound to comply with any data access request not later than 45 days of receiving the request. There are, however, certain circumstances where the data user may refuse to accede to the request of the data subject, where, for instance, disclosure would involve disclosure of information relating to another individual.[44]

When supplied with a copy of the personal data, the data subject has the right to correct personal data which he considers to be inaccurate.

The data subject also has the right to prevent collection, holding, processing or use of personal data that is causing or is likely to cause unwarranted damage or distress to him or another individual. This right is limited if the data subject has given his consent to the collection, holding, processing or use of the personal data or where the collection etc. is necessary in the prescribed circumstances.

Where data processing is done by automated means, the data subject has the right to require the data user to ensure that no decision taken by or on behalf of the data user which significantly affects that individual is based solely on the processing by automated means of the personal data.

[44] See clause 34 of the Proposed Bill.

Remedies of Data Subject

The data subject is entitled to compensation for any damage or distress suffered as a result of any contravention of any requirement under the Proposed Bill. Damage here includes injury to feelings.

The data subject is also entitled to complain to the Commissioner for Personal Data Protection of any contravention of a requirement under the Act. Such complaint may be made of a data user even though the data user may have ceased to be a data user provided that he has ceased being a data user during the period of two years immediately preceding the date on which the complaint was received. The Commissioner may on his own accord conduct his own investigations if there are reasonable grounds for him to believe that there is a contravention of a requirement of the Proposed Bill.

When the Commissioner is satisfied from his investigations that a data user has contravened or is contravening any of the data protection principles, he may serve the data user with an enforcement notice, directing the data user to remedy the contravention whithin a specified period.

It is a defence if the data user could show that he has taken care in all the circumstances and was reasonable to avoid any contravention or where the contravention occurred because of data inaccuracy, the data user accurately recorded the personal data received or obtained from the data subject or a third party.

Exemptions

Various exemptions from compliance with the above nine principles have been made with respect to the following : national security; crime and taxation; health; social work; regulatory functions; judicial appointment; legal professional privilege; domestic purposes; staff planning; relevant process; personal references; statistic and research purposes; news; sensitive personal data after death; and information available to the public by or under any written law.

It should be noted that 'exemptions' in this regard merely means that the data user need only comply with some, and not all of the nine principles stated above. For instance, in so far as personal data in a criminal investigation is concerned, the data user is exempted from

complying with principles 3, 4 and 7, which means the information collected could be used for any purpose or disclosed without the consent of the data subject, and the data subject could be denied access to and correction of data. In the Hong Kong case of *Tse Lai Yin Lily & Ors. v Incorporated Owners of Albert House*,[45] police took statements from witnesses in connection with an accident involving the collapse of a canopy. Subsequently, the plaintiff commenced an action against the defendant for damages for personal injuries from the accident. The police refused to release the statements for fear of violating the Hong Kong Personal Data (Privacy) Ordinance (Cap. 486). The issue was whether the use of the personal data would fall within the exemption under section 58(2) of the said Ordinance, which is similar to clause 73(1)(d) of the Proposed Bill, that is the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, or dishonesty or malpractices, by persons; and also principle 3 of the data protection principles, that is, data cannot be used for any purpose other than inter alia, a purpose directly related to the purpose for which it was collected. It was held that the word 'remedying' in section 58(2) extended the use of the personal data beyond criminal conduct to include civil wrongs. Further, the civil action was connected to the purpose for which the statements were taken.

Personal data collected for statistical and research purposes are expressly exempted from principles 3 and 4, although it remains a requirement not to use or disclose the data for any other purpose. There are only two categories under which there is total exemption from all nine principles, namely domestic purposes, and sensitive personal data after death.

Matching Procedure and Direct Marketing

Any proposed legislation on personal data would have an impact on data matching and direct marketing, and for this reason, provisions are made in the Proposed Bill to deal with these matters:

[45] [1999] 1 HKC 386.

Data matching is the comparison of two or more sets of records of individuals included in more than one database. The objective here is not the creation of a larger file of information about the data subject but the identification of anomalies or inconsistencies[46] in sets of data relating to the data subject for purposes such as the detection of fraud or the regulation or investigation into various activities. It does this by using a matching procedure to compare data held by different data users or by the same data user but for different purposes. An example of a comparison process is as follows: Data user A, who is responsible for selecting candidates who meet certain eligibility criteria for the award of a scholarship for tertiary education, collects and uses personal data on the candidates for the purpose of selection. One of the eligibility criteria is that the candidate must have been accepted as a student in one of the public universities. To check whether that eligibility criterion has been met, Data User A may compare his collected data with personal data collected by Data User B who selects candidates for entry into public universities. The comparison of the data held by Data User A with that of Data User B will confirm whether or not the candidate is eligible for the scholarship. Data matching is to a large extent facilitated by electronic records and distributive computing.

This process of comparison known as 'matching procedure' under the Proposed Bill is defined to refer to any procedure whereby personal data collected for one or more purposes in respect of ten or more data subjects are compared with personal data collected for any purpose in respect of the data subjects where the comparison for the purpose of producing or verifying data, or produces or verifies data in respect of which it is reasonable to believe that it is practicable that the data may be used, whether immediately or later, for the purpose of taking adverse action against any of the data subjects. "Adverse action" is defined as any action that may adversely affect an individual's rights, benefits, privileges, obligations or interests.

Data matching is seen to be posing threats to personal privacy as it involves analysing information about large numbers of people without

[46] Office of the UK Data Protection Registrar, *A Guide to Developing Codes of Practice on Data Matching* (1998).

prior cause for suspicion.[47] The Proposed Bill places various restrictions on matching procedures and requires any person proposing to carry out any matching procedure to seek consent from the Commissioner for Personal Data Protection.[48] It is an offence to carry out any matching procedure without the prior consent of the Commissioner. No adverse action resulting from the matching procedure is permitted to be taken unless the data user has served a notice on the individual specifying the adverse action proposed to be taken and the reasons and the individual has been given seven days to show cause why action should not be taken against him.

However, government departments, statutory bodies or local authorities are not required to seek the consent of the Commissioner although they are required to inform the Commissioner in writing that they are carrying out matching procedures. They are also not required to serve any notice that a person's data is being matched for comparison. It is not certain why these bodies are exempted especially when matching procedures are more likely than not to be used by government departments, statutory bodies or local authorities for various regulatory or investigative purposes. In view thereof some guidelines or procedure should be in place to assure individuals that they are not unfairly or discriminately being targeted for adverse action by the bodies or agencies concerned.

Direct marketing is defined to mean the offering of goods, facilities or devices, the advertising of the availability of goods, facilities or services, or the solicitation of donation or contributions for charitable, philanthropic, recreational, political or other purposes by means of information or goods sent to a person by mail, fax, email or other means of communication or by telephone calls.

---

[47] See the Australian Office of the Federal Privacy Commisioner at www.privacy.gov.au on data matching (last accessed 21 November 2003)

[48] There are various prescribed matters that the Commissioner would have to consider before acceding to any request for matching procedure. These include taking into account whether or not the matching procedure is in the public interest, the type of personal data involved, the consequences to the data subject of such procedures, the ability of the data subject to make a data correction request, and to verify the information, etc; see Third Schedule to the Proposed Bill.

A data user who uses personal data for direct marketing purposes is required to inform the data subject the first time he uses such data of the right of the data subject to request the data user to discontinue using his personal data if he so desired. If such a request is made, the data user must cease to use the personal data. This provision would appear to apply even if the data user has obtained the personal data for the purpose of direct marketing.

Transborder Flow of Personal Data

The Proposed Bill also addresses the issue of transborder flow of personal data. It prohibits and makes it an offence for any person to transfer personal data to a place outside Malaysia unless otherwise specified and gazetted by the Minister. There is no definition of 'transfer' but the word 'use' is defined to include transfer. In deciding whether to specify a particular country, the Minister must have reasonable grounds for believing that there is in that country a law that is substantially similar to and serves the same purpose as the Proposed Bill, or that the place ensures an adequate protection for the rights and freedoms of data subjects in relation to the collection, holding, processing or use of personal data. It is not certain why a permissive rather than a prohibitory approach was not proposed.[49] As it stands, unless and until specified by the Minister or exempted by statute, personal data may not be exported to any country. The proposed approach is cumbersome, impractical and will definitely act against trade. The requirement that the transfer would only be allowed by an order of the Minister may also prove to be impractical in the Internet environment, where information is transmitted across border and to any location en route its target destination.

Preferably the approach should be to allow for transfer unless it could be shown that the level of protection in the importing country is not adequate

[49] In this regard, the draftsman appears to have followed the approach of the Hong Kong Personal Data (Privacy) Ordinance (Cap 438): s 33. See, however, the UK Data Protection Act 1998 which provides that personal data shall not be transferred outside the European Economic Area unless that country or region ensures an adequate level of protection for the data: Sch 1.

It is also to be noted that the importing country must have a personal data law that is 'substantially similar' to the Malaysian law, or in the absence of such a law, an adequate protection for the rights of data subjects in so far as the collection, holding, processing or use of personal data is concerned.[50] The Proposed Bill does not define 'adequate' nor prescribe the criteria to be taken into account in assessing adequacy.[51]

The restriction on transborder data flows applies to all personal data collected, held, processed or used in Malaysia or which is controlled by a data user whose principal place of business is in Malaysia. The latter suggests that the restriction would apply even if the personal data was not collected, held, processed or used in Malaysia, which may have considerable impact on companies with their principal place of business located in this country.

However, there are circumstances under which such restriction does not apply, such as, where the data subject has consented to the transfer, or where the data user is exempted from principle 3. More important, the restriction does not apply in cases where the transfer is necessary such as for the performance of a contract between the data subject and the data user; for the conclusion of a contract between a data subject and a data user; for the pupose of, or in connection with any legal proceeding; for the pupose of obtaining legal advice; to protect the vital interest of data subject; or for reasons of public interest. The restriction does not apply where the data user has taken all rea-

[50] Art 25 of the EU Data Protection Directive provides for 'an adequate level of protection' only. See, however, s 33(3) of the Hong Kong Personal Data (Privacy) Ordinance, which refers to only a substantially similar law.

[51] See, however, Sch 1, Part 2, paras 13-15 of the UK Data Protection Act 1998, which provides that an adequate level of protection is one which is adequate in all circumstances of the case, having regard to factors such as the nature of the personal data, the country or territory of final destination of that information, the purpose for which and period during which data are intended to be processed, the law in force in the country in question, any relevant codes or conduct or other rules enforceable in that country or territory, and any security measures taken in respect of the data in that country or territory.

sonable precautions and exercised due diligence to ensure that the requirements of the proposed law would not be contravened in that place or where the recipient of data is subject to a binding scheme or contract to uphold requirements of the proposed law.

Concluding Remarks

The proposed law is significant as this is the first attempt by the Government to enact a law to deal with an aspect of privacy, albeit in a limited fashion. It attempts to address concerns of individuals in a world where their privacy is constantly being invaded and intruded upon without their knowledge or participation. With newer and more intrusive measures being undertaken in the aftermath of September 11, it has become even more imperative that such legislative responses are in place to ensure that the boundaries of individual privacy are not arbitrarily redefined. The policy of the Personal Data Protection Bill should ensure that the use of new information technologies sustains, and does not erode the protection of use, collection, and disclosure of personal information. The rights of the individual in relation to the collection, storage and dissemination of information concerning him must be secure and the individual must have the right to access and correct such information that is stored. At the same time, the law protecting these individuals cannot be so stringent that it restricts the ability of businesses to transfer personal information from one country to another. It is important to ensure a balance between the right of the individual to be protected and the ability of businesses to operate without undue restrictions.

Dr. Khaw Lake Tee*

* Professor
Faculty of Law
University of Malaya

WHO IS THE ULTIMATE PLANNING AUTHORITY IN MALAYSIA? REVIEWING THE POWERS AND ROLE OF THE APPEAL BOARD

Abstract

The Federal Constitution prescribes that town and country planning is a shared responsibility of the Federal and State Governments. The planning law in 1976 originally defined three levels of planning authorities all of them at the State level. This was expanded in 2001 to include a National as well as regional planning authorities. However, the quasi-judicial planning Appeal Board which is appointed by the State Government appears to be the ultimate authority since its decision is final and there is no power for the State or Federal governments to intervene. The Board is an innovation ahead of its time but its constitution lacks representation in relevant areas of expertise, power is concentrated on the Chairman and there are no apparent constraints on the scope and powers of the Board. A review of 12 years experience suggests that a restructuring of the Board should be carried to be more inclusive in its decision-making process. Its mandate and duty should be to protect environmental resources and public good rather than to serve private interests.

Introduction

The Malaysian planning law is closely modelled after the British counterpart. Its Town and Country Planning Act 1976[1] is substantially based on the Town and Country Planning Act 1970 of the UK[2] but

[1] *Town and Country Planning Act 1976* (Act 172) (Malaysia). This Act is referred to as the TCP Act 1976 in this article.

[2] Lee Lik Meng, Abdul Mutalip Abdullah and Alip Rahim, 1990, *Town Planning in Malaysia - History and Legislation* (Monograph, Universiti Sains Malaysia). Essentially, the Malaysian planning system created in 1976 is modelled on the Structure Plan /Local Plan system introduced in the 1970 Act of UK.