THE LAW REFORM COMMISSION OF HONG KONG

REPORT

REFORM OF THE LAW RELATING TO THE PROTECTION OF PERSONAL DATA (TOPIC 27)

August 1994

THE LAW REFORM COMMISSION OF HONG KONG

REPORT

REFORM OF THE LAW RELATING TO THE PROTECTION OF PERSONAL DATA

CONTENTS

Appendices

Introduction

Terms of reference

1. On 11 October 1989, under powers granted by the Governor-in-Council on 15 January 1980, the Attorney General and the Chief Justice referred to the Law Reform Commission for consideration the subject of "privacy." The Commission's terms of reference were:

> *"To examine existing Hong Kong laws affecting privacy and to report on whether legislative or other measures are required to provide protection against, and to provide remedies in respect of, undue interference with the privacy of the individual with particular reference to the following matters:*
>
> *(a) the acquisition, collection, recording and storage of information and opinions pertaining to individuals by any persons or bodies, including Government departments, public bodies, persons or corporations;*
>
> *(b) the disclosure or communication of the information or opinions referred to in paragraph (a) to any person or body including any Government department, public body, person or corporation in or out of Hong Kong;*
>
> *(c) intrusion (by electronic or other means) into private premises; and*
>
> *(d) the interception of communications, whether oral or recorded;*
>
> *but excluding inquiries on matters falling within the Terms of Reference of the Law Reform Commission on either Arrest or Breach of Confidence."*

2. This report only deals with (a) and (b). The remaining aspects of intrusion and interception will be dealt with in a later report.

What is privacy?

3. A key word in the terms of reference is "privacy". In a recent comprehensive review of the question, Professor Raymond Wacks concludes that "in spite of the huge literature on the subject, a satisfactory definition of

'privacy' remains as elusive as ever."[1] Similarly, the United Kingdom committee on Privacy ("The Younger Committee") concluded in its 1972 report that the concept of privacy could not be satisfactorily defined. The Younger Committee viewed its task as identifying the values in which privacy was a major element and then determining which of those values deserved protection.

4. This approach was also taken by the Australian Law Reform Commission in its 1983 report on privacy which noted:

> *"a valid approach in analysing privacy is to isolate and define the interests which are commonly grouped under the heading 'privacy interests' and to explore the extent of their legal protection."*[2]

5. The "interests" which the Australian Law Reform Commission thought invariably emerged in any discussion of privacy were:

(a) the interest of the person in controlling the information held by others about him, or "information privacy" (or "informational self-determination" as it is referred to in Europe);

(b) the interest in controlling entry to the "personal place", or "territorial privacy";

(c) the interest in freedom from interference with one's person, or "personal privacy;"

(d) the interest in freedom from surveillance and from interception of one's communications, or "communications and surveillance privacy".

6. Like the Younger Committee and the Australian Law Reform Commission, we have concluded that it is more productive to focus on the commonly agreed privacy interests rather than add yet a further definition of "privacy". Adopting the Australian analysis for this purpose, it will be apparent that item (a), namely "information privacy", corresponds to paragraphs (a) and (b) of our terms of reference. It is this aspect of privacy that is dealt with in this report.

7. It will be noted that the terms of reference refer to information and opinions relating to individuals. The nature of information about individuals varies enormously, from publicly available data such as names and addresses of telephone subscribers, to intimate data referring to an individual's sexual activities. For the purposes of this report "personal information" refers to any information relating to an identifiable individual,

---

1 Raymond Wacks, *Personal Information: Privacy and the Law* (Oxford, Clarendon Press, 1989), page 13.

2 Australia Law Reform Commission, *Privacy* (Report No 22), Canberra: 1983, page 21.

regardless of how apparently trivial it is. Information about intimate aspects of an individual's private life will be referred to as "sensitive information."

8. Other points worth noting about the terms of reference are:

(a) Whilst "information" is a readily understood term, this report will refer to "data" rather than "information." In particular, the internationally hallowed expression "data protection" will frequently recur. The literature tends to use "information" and "data" interchangeably, but it is important to note that strictly speaking "data" are wider than "information". The distinction has been put as follows:

> *"Information is not a thing, but a process or relationship that occurs between a person's mind and some sort of stimulus. On the other hand, data are merely a representation of information or of some concept. Information is the interpretation that an observer applies to the data."*[3]

Another commentator sums up the distinction by describing "data" as "potential information."[4] Because this report's concern is largely with information records, and also to accord with international usage, "data" will be used unless "information" is more apt. It should be stressed that this report is concerned only with *personal* data. All references to "data" are to "personal data".

(b) "Remedies" is wide enough to include, for example, complaints or conciliation procedures, as well as the conventional remedies of criminal or civil sanctions.

(c) "*Undue* interference" recognises that there are other considerations to be weighed against privacy interests, such as freedom of information and, at a different level, business efficiency.

(d) The reference is limited to the privacy interests of individuals. In our opinion, corporate and group claims to privacy raise complex issues distinct from those applicable to individuals and which would merit a separate reference.

Membership and method of work

9. The Law Reform Commission appointed a sub-committee to examine the current state of legal protection and to make recommendations.

---

[3] D. Piragoff, *Computer and Information Abuse: New Legal and Policy Challenges* (Department of Justice, Canada, 1989), page 4.

[4] Wacks, *op cit*, page 25.

The sub-committee was chaired by the Honourable Mr Justice Mortimer, a judge of the Court of Appeal and member of the Law Reform Commission. The other members of the sub-committee were:

Dr John Bacon-Shone	Director of the Social Sciences Research Centre, University of Hong Kong
Mr Don Brech	Former Director, Government Records Service
Mrs Patricia Chu	Assistant Director, Social Welfare Department
Mr Con Conway	Director of Community Affairs, Hong Kong Telecom
Mr Edwin C K Lau	Assistant General Manager, Retail Banking, Hong Kong and Shanghai Banking Corporation
Mr James O'Neil	Deputy Principal Crown Counsel, Attorney General's Chambers
Mr Jack So	Executive Director, Hong Kong Trade Development Council (resigned August 1992)
Mr Peter So	Deputy Commissioner of Police Management, Royal Hong Kong Police Force
Professor Raymond Wacks	Department of Law, University of Hong Kong
Mr Wong Kwok Wah	Managing Editor, Sunday Chronicle

10. The Secretary to the sub-committee was Mark Berthold, Senior Crown Counsel, who undertook the extensive research required by this project and on whom fell the considerable burden of drafting the sub-committee's report. We record here our appreciation of Mr Berthold's dedication to his task. We wish also to express our gratitude for the immense amount of hard work devoted to this complex project by the members of the sub-committee.

Consultation

11. Over the period of three years preceding the release of its Consultative Document in March 1993 the sub-committee reviewed the relevant legal and specialist literature in fifty-six meetings. This material highlights the international dimension of the protection of privacy. In order to discuss the issues with overseas experts, be they involved in the administration of privacy legislation or as commentators, members attended conferences in Amsterdam and Cambridge in 1991 and the 1992 International Data Protection Commissioners' Conference in Sydney (1992) and Manchester (1993). Officials from a number of other jurisdictions were met at these conferences, as were a number of internationally acknowledged academic experts, consultants and commentators. Members also visited the offices of the data protection authorities of the United Kingdom, Germany, the German province of Hesse, the Netherlands, Quebec, and Australia. We wish to express our gratitude to all those who met the sub-committee or supplied it with written material.

12. The sub-committee publicly released its interim proposals in a Consultative Document on 17 March 1993 and sought submissions from interested parties. The consultative period was twice extended and concluded on 1 August. Various professional associations arranged seminars featuring sub-committee members as speakers, including the Association of Banks, the Coalition of Service Industries, the Consumer Council and the Institute of Personnel Management. Members also attended District Board meetings to explain the proposals.

13. The consultation process elicited a large number of submissions. A list of these persons and organisations is at Appendix 1. With only three exceptions, the submissions received evince broad support for a data protection law applying to both the public and private sectors. The submissions detail those specific areas where respondents feared that practical problems might arise unless our proposals were modified.

14. We are grateful to all those who commented on the Consultative Document. Their contribution was invaluable in enabling first the sub-committee and then the Commission to refine the proposed scheme of data protection. The submissions were considered in detail and with considerable care by the sub-committee over the course of 20 meetings. This report contains references to, and extracts from, specific submissions where these are of particular relevance. Those references and extracts are necessarily selective (and restricted to those who did not object to such attribution in this final report) but it should not be thought that the absence of reference to a particular submission implies a lack of consideration: all were accorded careful examination.

The Commission Report

15. The sub-committee's final report was presented to the Law Reform Commission for discussion at its meeting on 24 May 1994. In view of the importance of the subject and the desire of both Government and public to see a final report as quickly as possible, a series of additional meetings were scheduled. In all, the Law Reform Commission considered the sub-committee's proposals in detail over the course of six meetings, the first of which was on 24 May and the last on 12 July 1994. Where our final recommendations differ from those in the Consultative Document we have endeavoured to make this clear.

Layout of the report

16. The body of this report commences with Chapter 1's brief overview of the information revolution to place the discussion in an empirical context. International developments are then examined in Chapter 2. The focus here is on the developing framework of human rights law and the initiatives of international organisations in developing data protection standards facilitating the burgeoning trade in personal data. We consider that these international standards provide the parameters for our proposed reforms. The existing legal framework in Hong Kong is examined in Chapters 3 and 4. Chapter 3 considers the extent to which domestic legislation currently affords protection to information privacy. It will be shown that apart from the privacy provision of the Bill of Rights Ordinance, scattered provisions provide only minor protection. Chapter 4 looks at the common law remedies developed by the courts, such as breach of confidence, which provide some protection to information privacy. Chapter 5 reviews the earlier chapters by asking to what extent statutory and common law provisions in Hong Kong currently implement international standards of information privacy protection. We conclude that they do so to only a limited extent and that as matters stand Hong Kong's legal system provides little protection to privacy. The remainder of the report comprises our recommendations seeking to remedy this situation. Each chapter commences with a summary. In the later chapters which contain recommendations, we set out the recommendations immediately after the summary.

Abbreviations

17. For the sake of brevity, when we refer to "he" we mean "he or she" unless the context implies otherwise. We refer throughout this report to a number of important papers and instruments. For the sake of conciseness, we use the abbreviated form shown below.

(i) "The OECD Guidelines"

The organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

(ii) "The ICCPR"

The International Covenant on Civil and Political Rights.

(iii) "The draft Directive"

The Commission of the European Communities amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

(iv) "The United Kingdom Act" or "The Act"

The United Kingdom Data Protection Act 1984.

(v) "The Council of Europe guidelines"

The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

(vi) "The BOR"

The Hong Kong Bill of Rights Ordinance (Cap 383).

(vii) "The Consultative Document"

The paper issued in 1993 by the Privacy Sub-committee of the Hong Kong Law Reform Commission, containing interim proposals on information privacy.

(viii) "The voluntary guidelines"

These are guidelines contained in a booklet entitled "Data Protection Principles and Guidelines" issued by the Hong Kong Government in March 1988.

Chapter 1

The information boom

Summary

1.1 Personal records have been with us as long as the written word but computerisation of them has become widespread only in the second half of this century. This development has revolutionised personal record keeping, because of the ease of storing, retrieving, combining and transferring data.

1.2 Computers have undergone a revolution of their own by evolving from large mainframes to microcomputers which are far more powerful than their larger predecessors. Properly used, these could significantly enhance the quality of human life but public concern has arisen about the privacy implications of the resulting large scale dissemination of personal data.

Computerisation and privacy

1.3 Manual records have been with us for centuries, but computers are a recent development. Computerisation has revolutionised record keeping. A 1975 United Kingdom White Paper[1] identified the following aspects of the operations of computers which have practical implications for privacy:

(a) they facilitate the maintenance of extensive record systems and the retention of data in those systems;

(b) they can make data easily and quickly accessible from many different points;

(c) they make it possible for data to be transferred quickly from one information system to another;

(d) they make it possible for data to be combined in ways which might not otherwise be practicable; and

(e) because the data are stored, processed and often transmitted in a form which is not directly intelligible, few people may know what is in the record or what is happening to it.

1.4 Initially, in the late 1950s and early 1960s, commercial computers were used mainly for mathematical and scientific calculations but

[1] Home Office, *Computers: Safeguards for Privacy*, Cmnd. 6354, 1975.

their use was soon extended to the management of large collections of data, known as "databases". Such data, including personal data, were stored in the then state-of-the-art mainframe/stand-alone computers. The operation of these very expensive computers was the preserve of specialists.

1.5 The current scene is very different. Technical progress has at once radically reduced the price and increased the performance of a new generation of microcomputers. These microcomputers have greater power and storage capacity than any mainframe of the 1970s. Their price/ performance ratio is thousands of times more beneficial to end-users than their monolithic predecessors. This has made them accessible to the public at large, facilitating their domestic use and, as the Council of Europe puts it[2], resulted in a gradual "banalisation" of data processing. Equally dramatic have been developments in telecommunications and its marriage with data processing which has revolutionised the circulation of data, including of course personal data. The centralised storage of data in one computer is giving way to the dispersal or distribution of a database amongst networked computers which are linked at will.

New sources of personal data

1.6 The new technology is also creating novel sources of personal data. One example is where a data user equipped with a terminal avails himself of such services as "teleshopping", "telebanking" and television programme requests. This generates personal data available to both the service provider and the carrier of the request, creating the potential for secondary uses. Another new source of personal data is provided by electronic funds transfer at the point of sale. This provides a record of a person's lifestyle as revealed by his purchase of goods and services with credit cards at networked terminals.

Anonymity and privacy

1.7 The commonly accepted equation of mass circulation of personal information with diminution of privacy does require scrutiny, however. Colin Tapper[3] points out that those processing personal data will know personally a much smaller percentage of the individuals to whom it relates than would occur in the earlier rural village environment. To this extent they will "care less about it", but the fact remains that they will base decisions on the data affecting the data subject. The impact of a decision to refuse a loan on the basis of a credit rating is not diminished by the fact that there is "nothing personal" intended concerning the anonymised data subject. Data protection laws are also concerned with fair information practices in a modern society.

---

2 Council of Europe, *New Technologies: A Challenge to Privacy Protection,* Strasbourg: 1989.

3 Colin Tapper, *Computer Law* (London: Longman, 1989).

Personal records and the control of behaviour

1.8 There is, however, an additional dimension involved in the uncontrolled acquisition of personal data. Although its original impetus is to record behaviour, it can become a force determining behaviour. Professor Flaherty pinpoints the potentially "chilling" effect of personal records on political behaviour in the following terms:

> *"The storage of personal data can be used to limit opportunity and to encourage conformity, especially when associated with a process of social control through surveillance. The existence of dossiers containing personal information collected over a long period of time can have a limiting effect on behaviour; knowing that participation in an ordinary political activity can lead to surveillance can have a chilling effect on the conduct of a particular individual."*[4]

1.9 The right to privacy is accordingly a condition necessary for the uninhibited exercise of other human rights such as free speech. Nor is only political behaviour susceptible to control. Professor Simitis[5] gives the following examples:

> *"The transparent patient". Computer programs designed by medical insurers to identify costly patients and accordingly to profile the ideal cost-saving patient, resulting in "an entirely transparent patient who becomes the object of a policy that deliberately employs all available information on her habits and activities in order to adapt her to insurers' expectations".*
>
> *"The righteous citizen." French, Norwegian and West German governments developed research programmes to identify deviant children who were then put in programmes to better adapt them to societal expectations.*

Inaccurate data

1.10 The technological sophistication of modern data processing does not guarantee the accuracy of the data recorded and disseminated. This is dependant on accurate inputting. If the data fed into the computer are inaccurate it will remain inaccurate but will acquire a greater potential to harm the data subject. It is therefore of concern that a number of studies have shown that personal data are often surprisingly inaccurate. David Burnham[6] provides a graphic example in the case of United States police records:

---

4 David Flaherty, *Protecting Privacy in Surveillance Societies* (University of North Carolina Press, 1989), page 9.

5 Spiros Simitis, "Reviewing Privacy in an Information Society", (1987) 135: 77 Penn Law Review 707.

6 David Burnham, *The Rise of the Computer State* (New York, Vintage Books, 1983), page 73.

"... the Office of Technology Assessment arranged for Dr Laudon to obtain access to a random sample of the criminal history records that recently had been dispatched to law enforcement and other agencies from five official repositories maintained and operated by three separate states and the FBI. The information in the records from the repositories was then compared with the information in the original records in files of the county courthouses. Procedures were followed that permitted the comparative analysis without disclosing individual names.

The findings are disturbing. In North Carolina, only 12.2 percent of the summaries were found to be complete, accurate and unambiguous. In California, 18.9 percent were complete, accurate and unambiguous. In Minnesota, the researchers found almost half the sample - 49.5 percent - met the same standards."

The scale of the problem

1.11 The result of these trends in the United States, to take one example, is summed up by the same author when he rhetorically asks:

"What does it mean, for example, that the officials and clerks of the US government, each year armed with more and more computers, have collected 4 billion separate records about the people of the United States, seventeen items for each man, woman and child in the country? What does it mean that an internal communications network serving just one multinational corporation now links more than five hundred computers in over a hundred cities in eighteen countries and has been growing at a rate of about one additional computer a week in recent years? What does it mean that ten thousand merchants all over the country are able to obtain a summary fact sheet about any one of 86 million individual Americans in a matter of three or four seconds from a single data base in Southern California?"[7]

Public concern about information privacy

1.12 The trends outlined above are common to industrialised countries. As Professor Simitis comments:

"It is, therefore, not surprising that opinion polls reveal a growing concern for individual privacy that clearly transcends national boundaries. In a 1982 poll conducted in Canada on public

[7] See Burnham, *op cit*, page 52.

attitudes toward computer technology, sixty-five percent of the persons surveyed identified invasion of privacy as their main concern. A year later, eighty four percent of those polled in the United States thought that a file containing credit information, employment data, phone calls, buying habits, and travel could easily be compiled. Also, in 1983, sixty percent of those surveyed in West Germany felt that computers have already given the state too many opportunities for control. Americans were more explicit. Seventy percent appear to be convinced that government will take advantage of the chances offered by technology in order to intimidate individuals or groups. Hence, both experience with the retrieval of personal data and the widespread distrust of those with access to personnel information systems demonstrate the universality of the problems created by intensive computerisation."[8]

1.13 Nor do data subjects now wait to be polled on the matter. A major consumer database developed by Lotus Developments and known as "Marketplace Households" was removed from the US market when 30,000 people telephoned or wrote requesting that they be removed from it. The product listed the names, income levels and spending habits of 120 million consumers on 11 compact discs accessible by an Apple Macintosh personal computer.[9]

1.14 To what extent these concerns are currently shared by Hong Kong people may be gauged to some extent by the only survey prior to our reference on the issue, in 1976.[10] A majority of the 355 residents randomly sampled responded that they "would object" to information "being made available to anyone who wanted it" relating to their address, telephone number, income, or financial assets. Surprisingly, they were less concerned about disclosure of their political or religious views, or their medical history - classes of information generally considered in developed countries to be particularly sensitive. A comparatively trustful attitude was also evinced regarding the administration's use of personal information. Of course, the political situation was more settled back in 1976, and computerisation was comparatively undeveloped. Fortunately, an independent survey was conducted during our public consultation period by the Social Sciences Research Centre at The University of Hong Kong, funded by the Conference & Research Grants Committee at the university. This survey was conducted by one of the sub-committee members (Dr Bacon-Shone) together with Dr Traver, the author of the 1976 survey. The survey covered four areas, namely breaches of personal privacy within the last year, what personal data is sensitive to public disclosure, situations requiring government control and demographic background of respondents. 1.5% of respondents had experienced a privacy invasion of great concern, which projects to more than 50,000 people in Hong Kong. Address and telephone numbers were

---

8 See Simitis, *op cit*, page 724.

9 *South China Morning Post*, 29 January 1991.

10 H. Traver, “Privacy and Density: A Survey of Public Attitudes towards Privacy in Hong Kong" (1976) 6 HKLJ 237.

regarded as overwhelmingly sensitive and the majority agreed that private photos, income, medical history, ID card number and HIV status were sensitive. Little concern was shown about political or religious views, or nationality. There was strong consensus that controls were needed to cover the availability of tax information, with some concern over credit checks and little concern regarding the unnecessary use of ID card numbers. There was overwhelming support for rights of access to, and correction of, personal data after a loan refusal. These attitudes were generally remarkably consistent across demographic boundaries and indicate public support for the principles of data protection, while recognising the necessity of business efficiency, such as in the use of ID card numbers. A summary of the survey results is at Appendix 2.

Automated and non-automated data mediums

1.15 A major initial decision which we have been required to make is whether automated and non-automated personal data should be treated identically. It is generally thought that automated records pose greater dangers to privacy, for the reasons given above, and some jurisdictions restrict the application of their data protection laws accordingly. Thus the Data Protection Act 1984 in the United Kingdom excludes non-automated data by defining "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". The fact that often the most sensitive information continues to be held on manual files has been recognised in that country, however, by subsequent enactments dealing with non-automated data held by social services, housing authorities and health workers. More fundamentally, the practical distinction between computerised and manual records is breaking down with the development of optical scanners and the cross referencing or tagging of the one medium to the other. We accordingly recommend below that both mediums be regulated. The details are set out later in this report and for present purposes it will suffice to observe that their increasing interrelationship obviates the need for a detailed comparison of the relative perils to privacy posed by computerised records on the one hand and manual records on the other.

Chapter 2

Information privacy in the international context

Summary

2.1 Two international aspects of information privacy of which local legal reforms must be cognisant are:

(i) internationally recognised data protection principles and the development and implications of transborder data flow regulation; and

(ii) the relevant law on human rights.

2.2 As to (i), guidelines have been developed by several international agencies. Our own recommendations are based upon the Organisation for Economic Co-operation and Development ("OECD") Guidelines, although the Council of Europe has also promulgated an influential and largely similar model. Twenty seven jurisdictions have data protection laws based upon one or other of these guidelines but there is increasing concern within the international community that the burgeoning cross border trade in personal data should not undermine progress. The developing trend is that countries lacking adequate data protection law will be denied general access to personal data from those possessing it. This is specifically envisaged by the Commission of the European Communities Commission draft Directive ("the draft Directive")[1].

2.3 Turning to (ii) above, the International Covenant on Civil and Political Rights ("ICCPR") applies to Hong Kong. Its privacy provision is the subject of general comment by the Human Rights Committee. Also, the European Court of Human Rights has interpreted this provision in two important decisions.

2.4 The ICCPR is narrower in scope than the OECD Guidelines. In particular, it affords protection only to information upon a person's private life. The privacy provision in the ICCPR has recently been incorporated into Hong Kong's domestic law with the enactment of the Bill of Rights Ordinance. The OECD Guidelines apply to any information relating to an identifiable individual. At present this provides the only enforceable right to privacy in Hong Kong. It is very limited in the absence of a Data Protection law.

---

[1] Commission of the European Communities "amended proposed for a Council Directive on the protection of individuals with regards to the processing of personal data and on the free movement of such data" (presented by the Commission pursuant to Article 149(3) of the EEC Treaty).

International formulation of data protection principles

Introduction

2.5 Whilst the rapid development of the new information technology has had a number of beneficial consequences, concerns about its privacy implications have occasioned several major international inquiries. These have resulted in the various formulations of the basic principles of personal data protection. Although they differ in their details, the various formulations have much in common. Before examining them, however, the background to their genesis will be looked at. This is to be found in the international exchange and flow of data, including personal data. Information is an essential commodity. It is obviously vital for Hong Kong to be equipped to participate fully in this trade if it is to secure its role as an international trading centre. It will be shown that Hong Kong's ability to do so will largely depend on the existence here of legislation that provides an adequate level of protection to information privacy. The developing trend is that those countries that do possess such laws will be increasingly cautious about transferring data to those countries that do not.

International trade in personal data

2.6 The increasing use of computers has coincided with a communications boom resulting in a massive increase in international data traffic. The transborder flow of personal data is generated where, for example, flight reservations are made in another country or foreign tourists use credit cards. Whilst a passenger will not be opposed to the transfer of data to another country to facilitate his flight, privacy issues arise if the data are used for other purposes, such as the marketing of other products to the passenger. Those countries that have already established data protection laws appreciate that privacy protection will be undermined by the unrestricted removal of data to other jurisdictions which lack such data protection standards (known as "data havens") for processing and storage. A large number of industrialised countries now possess data protection laws, and increasingly these laws restrict the transfer of data to countries lacking adequate data protection. This trend will inevitably accelerate in view of the requirements of the revised draft Directive. Presently expected to be brought into force in 1996, the draft Directive requires Member States to provide for restrictions on the transfer of personal data to third countries lacking an adequate level of data protection. The issue is considered in detail in Chapter 17.

2.7 A related situation is where the country from which data are transferred is concerned that the transfer is likely to lead to a contravention of the data protection principles. In his recent review of this issue,[2] Professor Joel Reidenberg comments:

---

[2] The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services", Fordham Law Review Volume LX, number 6, May 1992.

> *"National laws in Europe tend to allow or encourage the prohibition of data exports. In France, data processing activities involving the export of personal information must be registered with [the Data Protection Authority] and the Data Protection Authority has a discretionary power to prohibit transfers abroad of personal information. Ever since the French realized that dating service records might be sent overseas, the French have been particularly obsessed with fears that personal information would be exported from France to 'data havens' for processing."*

The United Kingdom Data Protection Registrar is empowered to prohibit such transfers and did so for the first time in December 1990 when prohibiting the transfer of personal data to named corporations in the USA.[3] The personal data comprised names and addresses for the purpose of direct mail. The United States had sought a court order in New Jersey to restrain the activities of the corporations in question, alleging that they were defrauding customers through false advertising (the order was granted).

2.8 It will be seen in Chapter 17 that methods are being developed aimed at providing a degree of assurance that the data protection principles will be applied to data transferred to a country which has not given those principles legislative force. Contract may provide such a mechanism. FIAT, for example, wished to transfer data on their French staff to headquarters in Italy, a country lacking a data protection law. The French data protection authority required FIAT-Turin to enter into a contract with FIAT-France undertaking to apply the data protection principles to the processing of the data in Italy.[4] The point to be made in the present context, however, is that such a contract would not have been required if the transferee country had possessed legislative protection of information privacy.

International initiatives to rationalise protection of information privacy

2.9 **OECD** The Organisation for Economic Co-operation and Development as its title suggests is primarily concerned with the economic development of its member states rather than with matters of human rights. Hence its concern is to balance personal information privacy interests with those of fair competition. The OECD membership is global, including not only many European countries but also the United States, Australia, New Zealand and Japan. In an effort to introduce a rationalisation of the international regulation of data flows, the OECD established in 1974 the first of two Expert Groups chaired by the Hon Mr Justice M D Kirby, then Chairman of the Australian Law Reform Commission. Those efforts culminated in a recommended set of draft Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. On 23 September 1980 the Council of the OECD resolved:

---

3 Stewart Dresner, "First UK Ban" *Privacy Laws & Business* Winter 1990/1991, page 5.

4 Adriana Nugter, *Transborder Flow within the EEC*, (Computer Law Series: Kluwer, 1990), page 204.

"that, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;

that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices;

that transborder flows of personal data contribute to economic and social development;

that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows;

Determined to advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries;

RECOMMENDS

1. That Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines contained in the Annex to this recommendation which is an integral part thereof;

2. That Member countries endeavour to remove or avoid creating in the name of privacy protection, unjustified obstacles to transborder flows of personal data;

3. That Member countries co-operate in the implementation of the Guidelines set forth in the Annex;

4. That Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines."[5]

2.10 The OECD Guidelines, although lacking legal force, represent a significant international consensus on the appropriate principles. The Explanatory Memorandum accompanying the OECD Guidelines explains that they apply to personal data in both the public and private sectors "which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties." Accordingly they are not restricted to automated data, unlike the Council of Europe convention discussed below. They define

[5] Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris: OECD, 1981.

"personal data" as "any information relating to an identified or identifiable individual (data subject)". The OECD Guidelines identify a number of "principles" as follows:

1. 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 or consent of the data subject.

2. Data Quality Principle

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

3. 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 of purpose.

4. Use Limitation Principle

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

(a) with the consent of the data subject; or

(b) by the authority of law.

5. 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.

6. Openness Principle

There should be a general policy of openness about developments, practices 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.

7. 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.

8. Accountability Principle

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

2.11 **United Nations Guidelines** In December 1990 the United Nations Commission on Human Rights adopted "Guidelines Concerning Computerised Personal Data Files." They comprise a set of data protection principles similar in their general scope to those of the OECD. In some important respects, however, they go further. For example, they explicitly recognise the need for the establishment of a supervisory authority.

2.12 **Council of Europe** Another body which has made a major contribution in determining the appropriate fundamental principles of data protection is the Council of Europe. Its involvement began in 1968 when the Parliamentary assembly of the Council of Europe expressed concern regarding the adequacy of article 8 of the European Convention of Human Rights to protect private interests in the computer age. It was thought that the right to respect for "private life" referred to by article 8 would not necessarily include all personal data and that the Convention had a defensive approach to privacy. It was thought that a more positive approach was required. The question was examined by a panel of experts and on 17 September 1980 the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was formally adopted by the

Committee of Ministers. In content, it has much in common with the OECD Guidelines, but unlike the Guidelines the Convention is legally binding and requires each State Party to take "... the necessary measures in its domestic law to give effect to the basic principles ...". The UK's desire to ratify the Convention provided the impetus for the enactment of the Data Protection Act 1984. That enactment sets out eight data protection principles which are based on the Convention. Data protection laws are generally structured around a set of data protection principles with much the same ambit as these two formulations, for despite variations in wording, there is basic agreement on what data protection principles are indeed "fundamental".

2.13 **Commission of the European Communities draft Directive** The latest chapter in international efforts to rationalise the legal protection of information privacy is being compiled by the Commission of the European Communities (the European Commission). On 18 July 1990 the European Commission issued a draft Directive concerning the protection of individuals in relation to the processing of personal data. The aim of the draft Directive is to harmonise the different data protection laws presently in force in the European Community, to ensure the free movement of personal data between Member States. The preamble notes that its proposals "give substance to and amplify" those contained in the Council of Europe Convention discussed above.

2.14 The initial draft Directive represented a "first bid". The European Parliament voted on a large number of amendments in March 1992. On 15 October 1992 the Commission issued a substantially revised proposal. The amendments provide for a more flexible and workable framework than its predecessor, whilst continuing to strive for a high level of protection. We have adverted to the revised draft Directive's proposals in formulating our own detailed recommendations on a data protection law.

2.15 **The data protection principles in Hong Kong** It will be seen below that in Hong Kong a set of data protection guidelines was issued in booklet form in 1988. The guidelines, which were approved by the Executive Council, are in similar terms to the major overseas models. They are intended for voluntary adoption by data users as they lack legal force.

Human Rights

Article 17 of the ICCPR

2.16 The ICCPR was ratified by the United Kingdom on 20 May 1976. Subject to certain reservations which do not pertain to privacy, the United Kingdom extended its application to Hong Kong on the same day. In so doing it undertook "to respect and to ensure to all individuals within its territory and subject to its jurisdiction" the rights recognised in the ICCPR (article 2(1)). The ICCPR does not constitute part of the domestic law as such but it requires States Parties "to adopt such legislative or other measures as may be necessary to give effect to the rights recognised in the ... Covenant" (article

2(2)). On 8 June 1991 the Hong Kong Bill of Rights Ordinance (Cap 383) ("the BOR) came into operation incorporating into domestic law the provisions of the ICCPR. As such, it is dealt with in Chapter 3's treatment of local legislation pertaining to information privacy. It is relevant in this context, however, to recall the legislative history of the Ordinance. The BOR only binds the government and public authorities. It provides no protection to the individual where his privacy is interfered with by another individual or private body. When first introduced, however, the Bill of Rights Bill contained a provision that would have imposed rights and obligations as between individuals. Following strong opposition, however, this provision was deleted. These objections were based on the concern that several rights in the BOR were expressed in very general language and their application in that form to the private sector would lead to difficulties. These concerns were shared by the Law Reform Commission's Privacy Sub-committee as regards the privacy provision set out below. It was thought that a more detailed regime was required in order to achieve certainty of application. The point was adressed by the Chief Secretary in his speech during the debate on the second reading of the Bill of Rights Bill.[6] Noting that the amended Bill removed all direct inter-citizen rights, he said that the question arose as to what alternative steps were required to supplement the BOR. Identifying privacy as an area where detailed private sector regulation was called for, he referred to the work of the Law Reform Commission in drawing up detailed proposals for legislation. This report represents the culmination of that process as regards data protection. Notwithstanding the enactment of the BOR, the ICCPR retains its status as an international treaty applied to Hong Kong. Accordingly the ICCPR is discussed at this stage in the context of the international dimension of the protection of information privacy. The analysis is also relevant, however, to the interpretation and hence operation of the domestic legislation incorporating its provisions.

2.17 Article 17 of the ICCPR provides a right to privacy in the following terms:

> *"1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
>
> *2. Everyone has the right to the protection of the law against such interference or attacks."*

2.18 It has been pointed out that "'No one' appears whenever the Covenant seeks to underscore a basic freedom which may not be denied to any person."[7] The scope of "unlawful" interference is reasonably clear, and "arbitrary" provides additional protection, as appears from a general comment of the Human Rights Committee. Before setting out the comment, its status will be briefly described.

---

6 Hong Kong Hansard, Session 1990/1 Volume 3, page 2337.

7 F. Volio, "Legal Personality, Privacy and the Family" in Henkin (ed), *The International Bill of Rights* (1981) Columbia University Press, page 185.

General comment on article 17 of ICCPR

2.19 Article 40(4) of the ICCPR provides that the Human Rights Committee may issue general comments on its provisions. The value of these comments is that they are formal statements more fully articulating the Committee's understanding of the legal content of the general language of the individual articles of the ICCPR. In *R v. Sin Yau Ming* the Hong Kong Court of Appeal considered the status of such comments when interpreting the identically worded provisions of the BOR. Silke V P there said that, although not binding on the court, he would "consider them as of the greatest assistance and give to them considerable weight."[8]

"Arbitrary interference"

2.20 The Human Rights Committee's general comment on "arbitrary interference" notes that it:

> *"can also extend to interference provided for under law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the [ICCPR] and should be, in any event, reasonable in the particular circumstances."*

Article 17 and information privacy

2.21 The application of article 17 to data protection may initially appear less obvious than it is to such activities as telephone tapping which fall under the rubric of communications and surveillance privacy. That it does so extend appears from the general comment of the Human Rights Committee on article 17, as well as several recent decisions of the European Court of Human Rights construing a similarly worded provision in the European Convention on Human Rights. It is paragraph 9 of the Committee's general comment on article 17 which deals with information privacy, the aspect of privacy which is the subject of this report. It states:

> *"The gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by states to ensure that information concerning a person's private life does not reach the hands of persons who are not authorised by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should*

[8] [1992] 1 HKCLR 127, at 141.

have the right to ascertain in an intelligible form whether, and if so what, personal data are stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination."

"Information concerning a person's private life"

2.22 It will be seen that this comment touches on matters such as data subject access which are dealt with more fully in the OECD Guidelines set out above. Those Guidelines in turn constitute the core of data protection legislation enacted in other jurisdictions. It would appear, however, that their scope is broader than the general comment in a fundamental respect. It will be recalled that the OECD principles define "personal data" to include any information relating to an identifiable individual. While the general comment does not specifically define the term, it refers to "information concerning a person's private life." This would appear to be narrower than the OECD Guidelines. It would presumably not usually encompass, for example, such publicly available details as one's address. While this narrower approach more closely corresponds to the intuitive concept of privacy, its rigid application is subject to fundamental difficulties. It may overlook the importance of context in determining the sensitivity of information. The address of an individual seeking refuge from an estranged and violent spouse is an example. It may also overlook the cumulative nature of data, whereby a personality profile may be compiled from a number of apparently innocuous details. It is not clear from the jurisprudence[9] whether or not the concept of "private life" is sufficiently flexible to accommodate these particular examples. For present purposes it will suffice to reiterate that "personal data" is broader under the OECD Guidelines than under the general comment on the scope of article 17.

2.23 Another difficulty in ascertaining the scope of the general comment resides in its focus on automated data, at least as regards access and correction rights. While we do not consider that the principles identified in the comment should be restricted to such data, the Committee has highlighted their application in that sphere. For the reasons given in Chapter 8, we see no fundamental reason in principle for distinguishing automated data from non-automated data which are readily retrievable through manual methods such as card indexes.

---

[9] See L. Doswald-Beck, "The Meaning of the 'Right to Respect for Private Life' under the ECHR" (1983) 4 *Human Rights Law Journal*, page 283. Also, A. Connelly, "Problems of Interpretation of Article 8 of the European Convention on Human rights" (1986) 35 *International & Comparative Law Quarterly*, page 567.

Relevant decisions of the European Court

2.24 The general comments of the Human Rights Committee quoted above relate specifically to the text of article 17 of the ICCPR. Also of relevance are two recent decisions of the European Court of Human Rights. These decisions turn on the privacy provision of the European Convention for the Protection of Human Rights and Fundamental Freedoms ("the European Convention"). Article 8 of this Convention provides:

> *"1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

2.25 We have set out this treaty provision to facilitate an assessment of the relevance of European Court decisions to article 17 of the ICCPR. It will be observed that, unlike the latter, the European Convention provision is not restricted to a protection against interference. On the other hand, article 17 does not include the European Convention's exception regarding interference necessary for national security, public safety, etc. This is not thought to be a difference in substance, however, as interference strictly justified by such reasons is unlikely to be "arbitrary" under article 17.

2.26 In *Leander v. Sweden*[10] the European Court of Human Rights held that there had been no breach of article 8 where secret information pertaining to an applicant for a security-sensitive post was consulted. For present purposes, the significant feature of the case is that the court held that this did constitute interference with privacy, although it was justifiable in the circumstances.

2.27 The facts of the case were that Mr Leander applied for employment in a naval museum, part of the premises of which were located within an adjacent naval base. His job application precipitated a security check consisting of consulting sensitive data held on a secret register held by the security police. In the result, Mr Leander was refused employment without being accorded an opportunity to see and to comment on the data released to the Navy from the secret police register. It was uncontested that the secret police register contained data relating to Mr Leander's private life and that both the storing and the release of such information, coupled with a refusal to allow Mr Leander to refute it, amounted to an interference with his right to respect for private life as guaranteed by article 8(1). The Court then had to

[10] (1987) 9 EHRR 433.

determine whether such interference was justifiable under article 8(2). This entailed balancing Sweden's interest in protecting national security against the seriousness of the interference with privacy.

2.28 The Court held that it was necessary for Sweden to have a system for controlling the suitability of candidates for security sensitive posts, provided there existed in such a system adequate and effective guarantees against abuse. The Court was satisfied there were such guarantees. They comprised the presence of parliamentarians on the police board that released the information to the navy as well as the supervision effected by the Chancellor of Justice, the Parliamentary Ombudsman and the Parliamentary Standing Committee on Justice.

2.29 *Gaskin v. United Kingdom*[11] is the most recent development in the European Court's information privacy jurisprudence. The Court there had to consider Mr Gaskin's complaint of continuing lack of access to the whole of his case file held by the Liverpool City Council. The facts were that following the death of his mother when he was one year old, the applicant was received into care of the Council and was boarded out with various foster parents, some of whom he contended mistreated him. The Court held that the personal file did relate to his "private and family life". It was not restricted to "personal data" in the general sense, but related to his basic identity, providing as it did the only coherent record of his early childhood and formative years. *Leander* was distinguished as that case was concerned with the negative obligations flowing from article 8(2), namely the guarantee against arbitrary *interference.* Mr Gaskin, however, did not complain of such interference, as he neither challenged the fact that information was compiled and stored about him nor alleged that any use was made of it to his detriment. His challenge related solely to the refusal to provide him with unimpeded access to that information and the Court considered that refusal could not be said to have interfered with Mr Gaskin's private or family life. The Court therefore had to examine whether the refusal of access constituted a breach of article 8(1)'s *positive* obligation of the right to respect for one's private and family life. The Court concluded that it did, apparently agreeing with the Commission that it required that everyone should be able to establish details of their identities as human beings without obstruction from the authorities.

2.30 Article 17 of the ICCPR does not impose an explicit positive obligation limb similar to article 8(1) of the European Convention; it appears to be solely concerned to provide protection against interference. (This does not entail denying that the concept of interference presupposes an affirmative right to respect to privacy, but merely notes that article 17 is expressly restricted to providing protection against interference with privacy.) In view of this, the Court's ruling that the positive requirement of article 8(1) had been breached as regards Mr Gaskin would appear to make the decision distinguishable when construing article 17 of the ICCPR. The relevance of *Gaskin* is that it further affirms that personal files may include data relating to "private and family life", an expression of similar import to "privacy, family,

[11] (1989) 12 EHRR 36.

home or correspondence" in article 17. Had there been evidence that the personal files had been used to Mr Gaskin's detriment, then this would have constituted "interference", the concept under article 17.

Article 19 of the International Covenant: privacy vs freedom of information

2.31 Article 19 of the ICCPR provides, in part

> *"...2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.*
>
> *3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:*
>
> *(a) For respect of the rights or reputations of others;*
>
> *(b) For the protection of national security or of public order (ordre public), or of public health or morals."*

2.32 It will be apparent from the above that there is an inherent tension between an individual's right to control information about himself and the rights of others to receive such information. The efficient functioning of government and commerce requires the disclosure of relevant personal information. The recurrent difficulty will be determining where to draw the line between these competing rights.

The ICCPR and the Basic Law

2.33 The Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China ("the Basic Law") was adopted at the third session of the seventh National People's Congress on 4 April 1990. It was promulgated the same day and is to come into effect on 1 July 1997. Article 39 refers to the ICCPR in the following terms:

> *" The provisions of the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights, and international labour conventions as applied to Hong Kong shall remain in force and shall be implemented through the laws of the Hong Kong Special Administrative Region.*

The rights and freedoms enjoyed by Hong Kong residents shall not be restricted unless as prescribed by law. Such restrictions shall not contravene the provisions of the preceding paragraph of this Article."

Competing interests

2.34 In specific situations other social interests will qualify the exercise of the right to privacy, just as freedom of information is restricted to protect national security, public health, etc. We address the issue in detail in Chapter 15 and recommend exemptions from a data protection law. In Chapter 18 we address the difficult issue of reconciling data protection and free speech rights of journalists.

Chapter 3

Hong Kong legislation and personal data privacy

Summary

3.1 Save for the Bill of Rights Ordinance (which applies only to the public sector) there is no specific legislative provision which provides for privacy of information. However, a number of ordinances regulate personal records held for diverse purposes such as education, employment, taxation, immigration, census and statistics, insurance, registration of persons and venereal disease. A brief account of the relevant provisions appears in this chapter. Not every such ordinance is identified, nor is there a comprehensive description of the relevant provisions. The aim is to provide an overview.

3.2 The ordinances are not uniform in approach but patterns can be discerned. Some require the data subject to provide information directly, whereas others which require the compilation of records do not expressly so stipulate.

3.3 Often authorities are specially empowered to obtain information from record keepers, but this power is usually (though not invariably) limited by a secrecy provision imposed upon the recipient. The ordinances with a secrecy provision are examined first, followed by those lacking it.

3.4 Further, in general these ordinances do not expressly sanction the transfer of personal information between governmental agencies.

3.5 In conclusion, there is a brief examination of the effect of the Bill of Rights upon information privacy in the public sector. Court decisions addressing the extent to which public authorities are permitted to pass on personal data are reviewed.

3.6 In considering the existing legislative framework, we note that in contrast to other jurisdictions, Hong Kong has no archives or records ordinance providing a statutory basis for the management of records by government agencies.

3.7 The practical application of data protection principles to government records requires effective and proper records management by all government agencies. This requires the maintenance, custody and disposal of records, irrespective of provisions in function-specific ordinances. Appropriate records standards should also be established.

Ordinances with secrecy provisions

3.8 Ordinances with secrecy provisions provide the highest degree of protection for personal information privacy and often accompany a statutory compulsion to provide information. The following are examples of ordinances with secrecy provisions.

Inland Revenue Ordinance

3.9 Section 51 of the Inland Revenue Ordinance (Cap 112) requires persons to furnish returns of their income. However, section 4 enjoins the Commissioner and his staff to preserve secrecy with regard to the affairs of any person coming to his knowledge in the performance of his duties. It prohibits him from communicating "to any person" (other than the taxpayer) any such matter, or providing him with access to departmental records or documents except in the performance of his duties. The legislation exhaustively spells out the exceptions to the secrecy requirement and the only excepted bodies are the Commissioner of Rating, other Commonwealth taxation authorities for tax relief purposes, the Director of Audit and the Attorney General in relation to tax appeals.

3.10 This provision or its equivalent is common in Commonwealth taxing statutes and has been judicially considered on a number of occasions. The extent of the judicial strictness evinced in these decisions is indicated by the ruling that the prohibition extends to communicating information to a court, on the basis that a court is a "person" within the meaning of section 4 (eg *Canadian Pacific Tobacco Co Ltd v. Stapleton*[1].

Census and Statistics Ordinance

3.11 Section 13 of the Census and Statistics Ordinance (Cap 316) requires persons to complete schedules relating to statistical inquiries. Whilst less comprehensive than the protection afforded by the Inland Revenue Ordinance, privacy is protected by several provisions. Section 6 requires census officers (defined to include the Commissioner) to complete a declaration of secrecy regarding information which they becomes aware of in the course of their duties. Sections 21 and 22 create offences in relation to the disclosure or publication of documents and information obtained under the Ordinance. Whilst reports may be published, they must be so arranged as to prevent the identification of particular individuals. The Census and Statistics (Amendment) Ordinance 1990 provides additional privacy protection by providing for voluntary statistical surveys. The latest census was conducted in March 1991 at an estimated cost of $180 million, a third of which was represented by a new computer system.[2]

---

1 (1952) 86 CLR 1.

2 *South China Morning Post*, 15 March 1991.

3.12 The Inland Revenue Ordinance and the Census and Statistics Ordinance both impose a statutory obligation on data subjects to disclose sensitive personal information. Their secrecy provisions can be viewed as encouraging the candour necessary if data subjects are likely to discharge this obligation. The legal compulsion to disclose one's affairs also has the potential to infringe the privilege against self-incrimination. A secrecy provision provides protection as regards other agencies.

Securities and Futures Commission Ordinance

3.13 An ordinance whose secrecy provision was relaxed in 1991 is the Securities and Futures Commission Ordinance (Cap 24). In a statement reported in the South China Morning Post on 19 April 1991 it was explained that section 59 inhibited the agency from fully co-operating with overseas regulators. It precluded, for example, the agency from providing information required by United Kingdom regulators if local brokers were to obtain full authorization in that country. The 1991 Amendment Ordinance authorises such disclosure provided that the recipient regulators are also subject to adequate secrecy provisions. Disclosure to the relevant agencies within Hong Kong is also authorised.

Immigration Ordinance

3.14 An example of an ordinance which compels data subjects to furnish personal information without the safeguard of a secrecy provision is provided by the Immigration Ordinance (Cap 115). Section 5 requires all arriving and departing persons to furnish a completed arrival or departure card. Section 14 requires aliens to furnish particulars and to advise of any change. Section 17 requires an alien to furnish information regarding his name, nationality, itinerary and occupation to persons providing him with rented accommodation. It is further provided that the recorded information is available for the use not only of immigration but also police officials. Section 17C requires all adults to carry proof of identity and to produce it on demand. Section 17K requires employers to keep records of employees' travel document details for inspection by immigration, labour and police officers. The Immigration Department is embarking on a $404 million computerisation programme with the "potential for future enhancement in capacity".[3] Upon completion, optical scanners will be installed to read identity cards and travel documents at checkpoints.

Rehabilitation of Offenders Ordinance

3.15 The Rehabilitation of Offenders Ordinance (Cap 297) is an interesting recent manifestation of increasing legislative awareness of

[3] *Hong Kong Standard*, 15 November 1991.

information privacy. It imposes restrictions on the disclosure of minor convictions where three years have elapsed without the convicted person being convicted again. Those restrictions provide for the inadmissibility of evidence of that conviction, the restrictive construction of questions relating thereto, and that the conviction or its non-disclosure is not a lawful ground for exclusion or dismissal of the convicted person from employment. Certain exceptions are prescribed. Disclosure of spent convictions is subject to criminal sanctions.

Insurance Companies Ordinance

3.16 The insurance industry is diverse and competitive. Insurers largely base their decision on whether to accept a risk on the information provided in the proposal form. The proposal form makes it clear that non-disclosure of information will, if material, avoid the policy. Particularly with life insurance cover, the life insurer may also require the proposer to sign a blanket authorization enabling the insurer to obtain information from any other source to verify the information provided by the proposer.

3.17 It is apparent that insurance companies hold a wealth of personal information, much of it of great sensitivity. Section 53A of the Insurance Companies Ordinance (Cap 41) provides that "except in the exercise of any functions under the Ordinance" (a recurrent expression in this context which will be examined below) persons appointed under the Ordinance shall preserve and aid in preserving secrecy with regard to all matters relating to the affairs of any insurer" acquired in the course of his duties. Limited exceptions are, as usual, prescribed. It should be noted that it is therefore the secrecy of the affairs of insurance companies and not those of insured persons which is in terms protected. This will provide a degree of incidental protection to those insured. But nowhere is there in the Ordinance any restriction placed on the insurance companies themselves as regards the disclosure of personal information relating to their customers. As discussed in the next chapter, however, they will be subject to common law restraints in this regard, namely those of contract and the duty of confidence.

Prevention of Bribery Ordinance

3.18 A provision which, were it not for judicial authority, might be thought to provide for secrecy is contained in section 30(1) of the Prevention of Bribery Ordinance (Cap 201). This provision makes it an offence to disclose "without lawful authority or reasonable excuse" to any person the identity of any person who is the subject of an investigation or any details of such an investigation. (The Prevention of Bribery (Amendment) Ordinance 1992 provides that the subsection does not apply following arrest). The section was considered in *Hall v. ICAC*[4]. The decision of the Court of Appeal has general implications for the exchange of personal information and is

[4] [1987] HKLR 210.

examined below. For present purposes it is sufficient to note that it was held that when the Independent Commission Against Corruption ("ICAC") passed on evidence to the Jockey Club for the purpose of disciplinary proceedings it did so with "lawful authority or reasonable excuse".

Banking Ordinance

3.19 The Banking Ordinance (Cap 155) possesses a secrecy provision (section 120) regarding the affairs of persons coming to the knowledge of a public officer or other person specified in section 120(2) in the course of his duties. Until its amendment in 1990 the secrecy provision was restricted to companies and did not apply to individuals. The amendment usefully supplements the common law protections afforded customer confidentiality described in the next chapter.

Other ordinances with secrecy provisions

3.20 The Commissioner for Administrative Complaints Ordinance (Cap 397) is a further example of legislation containing a secrecy provision. Section 15 requires the Commissioner and his staff to maintain secrecy in respect of all matters that come to their actual knowledge in the exercise of their functions, except in order to disclose an offence under the ordinance, evidence of a crime, or in relation to a breach of secrecy. Similarly, the Judicial Service Commission Ordinance (Cap 92) prohibits members from disclosing information (much of which will be sensitive) to those not authorised to receive it. Another example is the Money Lenders Ordinance (Cap 163). The officials administering this Ordinance and investigating such matters as excessive interest rates are subject to an obligation of secrecy imposed by section 5. Section 77 of the Credit Unions Ordinance (Cap 119) makes it an offence for a credit union officer to disclose any information regarding a transaction of a member except insofar as it is necessary for the proper conduct of the business.

Ordinances dealing with family data

3.21 Family relationships are obviously a source of sensitive personal information and this has been accorded a degree of legislative recognition. Thus, section 18 of the Adoption Ordinance (Cap 290) provides that the records associated with adoption shall not be open to public inspection, nor should extracts be furnished, except pursuant to a court order. Similarly, rule 121 of the Matrimonial Causes Rules (Cap 179) requires leave of the court for access to registry documents relating to orders not made in open court.

Legislation abrogating secrecy

3.22 There is an increasing legislative trend to enact legislation abrogating secrecy for such public purposes as the detection of crime. Section 67 of the Police Force Ordinance (Cap 232) requires banks and deposit taking companies to furnish information regarding a customer whom the police reasonably suspect of having committed an indictable offence. A court order is not required under the provision. Rather, the duty to furnish the information arises upon receipt of the Commissioner's request in writing. Failure without reasonable excuse to comply with the notice is a criminal offence. Section 14(1)(f) of the Prevention of Bribery Ordinance (Cap 201) is wider and empowers the ICAC to require "the manager of any bank to give to the investigating officer specified in such notice copies of the accounts of such person or of his spouse, parents or children at the bank". Unlike the position under the Police Force Ordinance, the duty to furnish this information arises upon receipt of a notice in respect of an "alleged or suspected" offence. A reasonable suspicion is not required. Section 20 of the Evidence Ordinance (Cap 8), however, requires a court order to compel the production of a banker's record as evidence in court where the bank is not a party to the proceedings. Section 13(2) of the Independent Commission Against Corruption Ordinance (Cap 204) is cast in wide terms and provides that the Commissioner, for the purpose of the performance of his functions, "shall have access to all records, books and documents relating to the work of any Government department in the possession of any Crown servant". The Drug Trafficking (Recovery of Proceeds) Ordinance (Cap 405) is a recent additional measure which not only abrogates the duty of confidence but statutory secrecy provisions as well. The legislation provides for the tracing, confiscation and recovery of the proceeds of drug trafficking. A court may order that material, including computerised information, be made available to investigating officers if the court is satisfied that:

(i) a specified person has benefitted from trafficking;

(ii) there are reasonable grounds for believing the material is substantially relevant, and;

(iii) it is in the public interest that access to the material should be granted.

3.23 Applications for disclosure of information held by public bodies are dealt with by the High Court under a separate procedure. Section 23(9) of Cap 405 provides that "material may be produced or disclosed in pursuance of this section notwithstanding any obligation as to secrecy or other restriction upon the disclosure of information imposed by statute or otherwise". This operates to override the secrecy provisions described above, including section 4 of the Inland Revenue Ordinance.

Disclosure in the performance of an officer's duties

3.24 Secrecy provisions invariably include an exception where the disclosure occurs in the performance of the officer's duties or functions, or

words to that effect. These words in a secrecy provision have been given a broad interpretation in the High Court of Australia decision of *Canadian Pacific Tobacco Co Ltd v. Stapleton*[5]. The court there held that:

> *"… the words 'except in the performance of any duty as an officer' ought to receive a very wide interpretation. The word 'duty' there is not, I think, used in a sense that is confined to a legal obligation, but really would be better represented by the word 'function'. The exception governs all that is incidental to the carrying out of what is commonly called 'the duties of an officer's employment', that is to say, the functions and proper actions which his employment authorises."*

3.25 The exception provision in the Inland Revenue Ordinance is slightly different, as it refers to the "performance of his duties under this Ordinance" rather than "performance of any duty as an officer". But, if adopted, this approach would arguably countenance, for example, Inland Revenue Department staff providing their files to ICAC officers investigating allegations of corruption involving an offence against the Ordinance or some attempted fraud to deprive the revenue of tax. It would not, however, authorise IRD staff providing their files to the ICAC or police to facilitate the latter's general investigation of corruption or crime. This is because the Inland Revenue Ordinance contains a number of express provisions establishing the criteria for tax liability and the mechanisms for revenue collection, as opposed to some broad statutory mandate such as to "obtain revenue". A great number of further functions and duties of IRD staff must be implied if the Ordinance is to be enforced but it is not possible to fix onto any of these express or implied provisions an "incidental or consequential" duty to disclose a taxpayer's affairs.

Disclosure of data under ordinances lacking secrecy provisions

3.26 Most ordinances which are likely to generate personal data lack secrecy provisions. There is no discernible pattern in the approach taken. Some ordinances impose an express duty on the authorities to compile records. Other ordinances (the Prevention of Bribery Ordinance (Cap 201) is an example) are silent on the point, no doubt on the reasonable assumption that the necessary records will be compiled in any event. In the case of the Police Force Ordinance (Cap 232) it is left to the Police General Orders to spell out (in great detail) what records are to be compiled. The ordinances also differ on the extent to which they expressly sanction an authority disclosing information to another authority.

---

[5] *op cit.*

Employment Ordinance

3.27 In Hong Kong, the majority of adults are employed in the private sector and in practice an employer may require all such personal information as he sees fit. Much of this information will be recorded. The Employment Ordinance (Cap 57) requires the recording of certain matters, namely maternity leave (section 15B), the date of commencement and termination of employment (section 37), annual leave (section 41G), and detailed employment histories including the employee's identity card number, job title, and wages (section 49A). Nor is the information net extended solely to employees, for section 56 requires employment agencies to maintain records and furnish returns. Section 58 of the Ordinance confers wide powers on the Commissioner regarding the inspection and copying of the records of employment agencies.

Education Ordinance

3.28 Another sector of activity which generates detailed personal records, including much sensitive information, is the education system. As with employment records, records generated by the education system cover most of the population. They vitally affect career prospects. Despite this, the meagre reference to personal records in the Education Ordinance (Cap 279) affords educators almost unfettered freedom to compile such records as they see fit. The matter is left to regulation 90 of the Education Regulations which simply provides that "a separate attendance register in a form approved by the Director shall be kept for each class". The disclosure provision is, however, much broader as it states that "the supervisor shall submit to the Director, whenever required by the Director, such information concerning the school or pupils thereof as may be required by the Director" (regulation 94). This provision does not purport to exhaustively define the circumstances in which teachers may pass on personal information. It was recently reported that a study is being commissioned by the Education Department to examine the feasibility of a system whereby schools will be able to access the Head Office computer. This computerisation project was expected to be the biggest yet undertaken by a government department.

Registration of Persons Ordinance

3.29 The Registration of Persons Ordinance (Cap 177) provides for the issue of identity cards, each of which is coded with a unique personal identifying number or "PIN". The Ordinance imposes a duty on every registered person in all dealings with Government to furnish the PIN if requested. PIN's facilitate the matching of diverse records relating to the individual identified by the PIN. This fundamental problem is addressed in Chapter 11 by specific data protection proposals. For present purposes it is sufficient to note that neither the Ordinance nor its regulations stipulate any legal protection against abuse. On the other hand, the regulations empower the Commissioner "to keep such records as he may consider necessary,"

including details of name, residential and business address, claimed nationality, place of birth, date of birth gender, marital status, names, ages and gender of children, occupation, details of travel documents and, in the case of persons entering Hong Kong, details of every country he has resided in for 6 months prior to entering Hong Kong (regulations 4(1) and 8(1)). Absent from the legislation is any provision restricting the disclosure of this personal information. Regulation 24 of the Regulations, however, does prohibit registration officers from producing or supplying copies of a registered person's photograph or particulars without the permission of the Chief Secretary (which may, however, relate to classes or categories of persons). They are also required to destroy the photographs or recorded particulars when they are no longer required.

Ordinances dealing with health data

3.30 The Venereal Disease Ordinance (Cap 275) deals with sensitive personal information and requires its disclosure in the interests of public health. Section 3 imposes a duty on medical practitioners upon receiving information from the patient as to the identity of a suspected source to report both to the Deputy Director of Health. Persons suspected of being infected by at least two patients may be sent an examination notice which is required to be personally served unless all reasonable attempts to do so are exhausted. Similarly, the Prevention of Spread of Infectious Diseases Regulations (Cap 141) require medical practitioners to report suspected cases of infectious diseases to the Director of Health (incidentally, neither ordinance applies to the AIDS virus). There is at present no Hong Kong legislation dealing with the disclosure of patient-identifiable confidential information in medical research. The doctor/patient confidential relationship will be examined in the next chapter dealing with common law doctrines pertaining to privacy.

Legal Aid Ordinance

3.31 Another professional relationship which has a confidential aspect is that of solicitor and client. Section 24 of the Legal Aid Ordinance (Cap 91) provides that the like privileges and rights as arise from the relationship of client, counsel and solicitor apply in the legal aid context, except "in relation to any information tendered to the Director concerning the property or income of the applicant for a legal aid certificate." This falls far short of section 22 of the United Kingdom Legal Aid Act 1974 which imposes a duty of secrecy without any similar qualification.

Societies Ordinance

3.32 The Societies Ordinance (Cap 151) requires any organised group to notify the Societies Officer of its establishment and supply certain particulars. Section 15 empowers the Registrar to require any society to furnish him with such information as he may reasonably require for the

performance of his functions. This is narrower than the previous formulation of this provision, which expressly authorised the Registrar to require a complete list of all members (the names of office bearers must still be provided). This is important, given the absence of a provision restricting the Registrar's power to disclose this information acquired under the legislation.

Electoral records

3.33 The Electoral Provisions (Registration of Electors) Regulations (Cap 367) and the Legislative Council (Electoral Provisions) (Registration of Electors and Appointment of Authorised Representatives) Regulations (Cap 381) provide for the compilation of detailed registers of electors. Details of electors included are identity card number, name, sex and residential address. The final registers are available for public inspection free of charge at offices identified by gazetted notices published in the daily newspapers (one English language and one Chinese language).

Ordinances requiring disclosure of financial interests

3.34 There are a number of ordinances which require persons to disclose financial interests where there arises a potential conflict of interests. Examples are provided by section 162 of the Companies Ordinance (Cap 32) and the Securities (Disclosure of Interests) Ordinance (Cap 396).

Other ordinances dealing with personal records

3.35 Other ordinances dealing with the keeping of personal records include the Detention Centres Regulation of Offenders Rules (Cap 298), and the Training Centres Regulations (Cap 280). Records are also kept of children in child care centres under the Child Care Centre Regulations (Cap 243).

The United Kingdom Official Secrets Act 1989

3.36 This Act was applied to Hong Kong in 1992. It plays an equivocal role in the protection of privacy. It replaces the 1911 Act, section 2 of which made it an offence for a person who obtains information in his official capacity to disclose it without authority. The breadth of the provision was commonly illustrated by the example of a civil servant disclosing how much tea is consumed in his canteen. The Official Secrets Act 1989 repeals section 2, thereby abolishing the general offence of disclosure of official information. Instead, it distinguishes between different categories of information. It is now an offence to disclose official information only if it relates to the security services, defence, international relations or crime prevention and detection and then generally only where the disclosure damages certain interests. The Act enhances one aspect of information privacy, insofar as it inhibits public

officers from divulging without authority personal information to others. Such authority could be expected to be more readily implied with disclosures within the civil service than to members of the public.

3.37 Whilst the Official Secrets Act operates to inhibit the disclosure of information (including personal information) without authority, it negates another aspect of information privacy. That is the aspect embodied in the data protection principle (the OECD Individual Participation Principle referred to above) that an individual have communicated to him data relating to him. In the United Kingdom this right is provided, subject to limited exceptions, by the Data Protection Act 1984. This report recommends that Hong Kong also enact a data protection law.

Permissible limits to disclosure by public authorities of information acquired under statutory powers

3.38 In their *On the Record: Surveillance, Computers and privacy*,[6] Campbell and Connor allege that in the United Kingdom personal information is freely swapped between government departments. A similar practice could exist in Hong Kong. We have seen that some legislation expressly prohibits disclosure but such secrecy provisions are comparatively rare. Nor is it usual for legislation to expressly authorise the passing on of information obtained pursuant to statutory powers. The Hong Kong Court of Appeal considered the issue in *Hall v. ICAC*[7]. The facts were that Hall, a jockey, had been investigated by the ICAC. Records were seized and he was interviewed. No criminal charges resulted but the ICAC forwarded to the Royal Hong Kong Jockey Club a file of evidence against Hall. The Jockey Club subsequently informed Hall that he would face disciplinary proceedings. On an application for judicial review, Hall sought declarations to the effect that it was unlawful for the ICAC to pass on the evidence against Him. Two of the judgments delivered differ in their approach. The third judge simply expressed agreement with both. Cons V P concluded that although there was no express statutory sanction in the ICAC Ordinance for the passing on of the information, the Ordinance read as a whole evinced the legislative intention that it be passed on in the circumstances of this case. In the words of the judge:

> *"... where the Commissioner has evidence of a corrupt practice that does not fall within the ambit of [specific] offences, but is within the jurisdiction of some body other than the court, then it is the intention of the legislature that the Commissioner should have the authority to refer that evidence to the particular body to take such action as it can with a view to reducing or eliminating corruption generally within Hong Kong."*[8]

---

6 London: Michael Joseph (1986).

7 *op cit.*

8 *ibid*, at 216.

This approach means that determining whether an ordinance permits an authority to disclose personal information to another authority is an exercise in statutory interpretation. If there is an express statutory sanction (many examples have been given above) then the answer is clear. If not, then a statute may nonetheless evince implied permission for disclosure. The principle appears unexceptionable, if often difficult and uncertain in application. It is worth bearing in mind in this context section 40 of the Interpretation and General Clauses Ordinance (Cap 1). That provides:

> *"Where any ordinance confers upon any person power to do or enforce the doing of any act or thing, all such powers shall be deemed to be also conferred as are reasonably necessary to enable the person to do or enforce the doing of the act or thing."*

3.39 The other leading judgment in *Hall* articulates a principle which is much more definite in its application, but is also much more susceptible to criticism. Fuad J A also held that the ICAC had implied powers to disclose such information, but went on to hold that:

> *"Apart from the import of language, no authority was cited to us ... that demands that there be specific statutory authority before there can be disclosure of information lawfully obtained. The reverse is the position in my view, and there would have to be express provision on the lines, for example, of section 4 of the Inland Revenue Ordinance (Cap 112) or section 22 of the Census and Statistics Ordinance (Cap 316) to prevent disclosure by the Commissioner, and thus to avail Mr Hall."*[9]

The two provisions referred to are the secrecy provisions discussed earlier.

3.40 The judgment of Fuad J A puts into practice the comment of Sir Robert Megarry V C in *Malone v. Metropolitan Police Commissioner*[10]*:*

> *"England it may be said, is not a country where everything is forbidden except what is expressly permitted: it is a country where everything is permitted except what is expressly forbidden."*

3.41 This proposition is cited with approval by Cons V P as "a basic premise" which applies also to Hong Kong, but he does not rest his decision on it. The proposition overlooks a number of distinctions that the law draws between public authorities and private individuals[11].

3.42 *Hall was* followed in *Ho Shan Hong v. Commissioner of Police*[12]. Whilst both decisions may be correct on their facts, they should now be considered in the light of the recent English Court of Appeal decision of

---

9 *op cit*, at 219.
10 [1979] 1 Ch 344.
11 H.W.R. Wade *Administrative Law* 6th edn; (Oxford University Press), pages 399-400.
12 (1987) HKLR 945.

Marcel v. Commissioner of Police[13]. Although the court there held that the police were liable to produce to a court on a subpoena documents seized under statutory powers, it considered that strict limits must be placed on their voluntary disclosure as they were subject to a duty of confidence.

3.43 The ruling arose from a motion for injunctions restraining the police from disclosing to third parties documents obtained without a search warrant pursuant to statutory search and seizure powers. The material had been obtained in the course of an investigation of alleged criminal offences but before any charges had been brought the police were served a subpoena to produce the documents in a civil action involving different parties. The *Malone* principle that everything is permitted which is not expressly forbidden was cited and it was argued that as there was nothing in the legislation to prohibit disclosure it must be permissible. To this Sir Christopher Slade rejoined:

> *"In my judgment, however, there is another principle of English law more relevant to the particular facts of the present case. As the [Judge below] pointed out 'search and seizure under statutory powers constitute fundamental infringements of the individual's immunity from interference by the state with his property and privacy-fundamental human rights'. In my judgment, documents seized by a public authority from a private citizen in exercise of a statutory power can properly be used only for those purposes for which the relevant legislation contemplated that they might be used. The user for any other purpose of documents seized in exercise of a draconian power of this nature, without the consent of the person from whom they were seized, would be an improper exercise of the power. Any such person would be entitled to expect that the authority would treat the documents and their contents as confidential, save to the extent that it might use them for purposes contemplated by the relevant legislation ... I cannot accept Mr Serota's broad submission that the powers of retention conferred on the police ... can properly be exercised for any purposes which are reasonable from a public point of view."*[14]

3.44 In its report on *Breach of Confidence,* the English Law Commission concluded that where information is supplied to public authorities but:

> *"is not given voluntarily, either because it way acquired by or under some statute or to the extent that it was given in order to receive a benefit or permission by or under statutory powers, it is not clear that the courts would spell out an obligation of confidence on the part of the recipient."*[15]

---

13 [1992] 1 All ER 72.

14 *ibid,* at 86.

15 Law Commission, *Breach of Confidence*, Cmnd 8388, paragraph 5.31.

3.45 *Marcel* has now spelt out an obligation as regards information acquired under statutory powers. Dillon L J specifically adverted to the point, saying that the duty of confidentiality "arises from the relationship between the parties. It matters not, to my mind, that in this instance, so far as the owners of the documents are concerned, the confidence is unwillingly imparted." While that decision involved comparatively draconian search and seizure provisions, there is no reason in principle why the obligation may not extend to information imparted in order to receive a benefit or permission.

3.46 It will be recalled that the OECD Guidelines (the Purpose Specification and Use Limitation Principles) require that 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 those purposes. The free exchange among public authorities of personal information is inconsistent with the Purpose Specification and Use Limitation Principles. As the judge at first instance put it in a passage approved by the Court of Appeal in *Marcel:*

> *"There are today numerous agencies of the state upon which, no doubt for good reason, Parliament has conferred the power compulsorily to obtain information and documents from the private citizen. If this information is not communicated to others but is known to, and used by, only the agency which is given the statutory power to obtain it, no great harm is done. But if the information obtained by the police, the Inland Revenue, the social security offices, the health service and other agencies were to be gathered together in one file, the freedom of the individual would be gravely at risk. The dossier of private information is the badge of the totalitarian state."*

3.47 We agree with these concerns and note that under the doctrine of precedent decisions of the Hong Kong Court of Appeal are binding on that court and on inferior courts in the territory: *Ng Yuen-shiu v. Attorney-General*[16]. The court is not bound by decisions of the English Court of Appeal: *de Lasala v. de Lasala*[17]. The Bill of Rights affects matters but we consider that legislative intervention is desirable to resolve the situation and believe that our detailed recommendations set out below address the problem.

Bill of Rights Ordinance

Enacted in 1991, the Bill of Rights Ordinance (Cap 383) ("the BOR") incorporates into Hong Kong's domestic law the provisions of the ICCPR, with some minor variations and qualifications. Fully incorporated is the ICCPR's privacy provision (article 17), which is duplicated as article 14 of the BOR. The BOR only binds the government and public authorities. This restriction is further examined in Chapter 5. It is not, however, relevant to the present issue of the statutory constraints rendering unlawful governmental

---

16 [1981] 1 HKLR 352.

17 [1979] HKLR 214 (PC).

disclosure of personal information acquired in the exercise of its statutory powers.

3.48 Article 14 of the BOR provides:

> *"Protection of privacy, family, home, correspondence, honour and reputation*
>
> *(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
>
> *(2) Everyone has the right to the protection of the law against such interference and attacks."*

3.49 Chapter 2 discusses the treaty counterpart to this provision, namely the identically worded article 17 of the ICCPR. We there analyse the relevant decisions of the European Court of Human Rights. We also set out the general comment of the Human Rights Committee elaborating on the article's scope. The full text of the comment is set out at paragraph 2.21 above. Of particular relevance to the present issue are the words:

> *"Effective measures have to be taken by states to ensure that information concerning a person's private life does not reach the hands of persons who are not authorised by law to receive, process and use it ….. "*

3.50 On this basis, it is arguable that it would constitute a breach of the BOR for a public authority to disclose information "concerning a person's private life" in the absence of express statutory authority sanctioning the disclosure. We saw earlier that the quoted expression has a narrower ambit than any information relating to an identifiable individual. As regards information concerning a person's private life, the application of the general comment would have the effect of subjecting the various ordinances detailed above to a test similar to that enunciated in *Marcel,* and accordingly narrower than that stated in *Hall.*

3.51 There have been no judicial decisions on the application of article 14 of BOR to the disclosure of information. However, in *R v Securities and Futures Commission, ex parte Lee Kwok-hung*[18], the Court of Appeal ruled that certain investigative powers of the Securities and Futures Commission were consistent with article 14, having regard to the need to balance the interests of the individual and of society. However, the Judges differed on the interpretation of the terms "unlawful" and "law" in article 14, with one expressing the view that they were not restricted to the domestic law of Hong Kong but encompassed, in addition, a "universal concept of justice",

[18] (1993) 11 HKLR 51.

whilst another thought that the terms referred only to that law which is found in relevant statutes or in the common law.

Access to Information Bill

3.52 The publication for public consultation earlier this year by Legislative Councillor Christine Loh of a draft Access to Information Bill prompted an extensive debate on the questions involved. Though distinct from data protection, access to information legislation clearly impinges on some of the same issues. The sub-committee considered the draft Bill as it affected the proposed data protection regime. On 8 March 1994, the sub-committee met Ms Loh and discussed the Bill. The briefing paper prepared for that meeting is annexed at Appendix 3.

Chapter 4

Common law principles protecting privacy

Summary

4.1 In addition to the limited protection of information privacy provided by local legislation which was described in the previous chapter, the common law provides some protection. Two aspects of the common law are examined in particular in this chapter:

(i) breach of confidence, which provides the greatest degree of protection to privacy, imposes an enforceable obligation on a person to whom information is disclosed for a limited purpose. Two confidential relationships which illustrate the duty of confidence are examined in detail, namely those of doctor/patient and banker/customer; and

(ii) the legal protection against unauthorised disclosure provided by the law of contract, either by express or implied terms in the contract.

Other relevant legal principles which are examined in this chapter are public interest immunity, legal professional privilege, copyright, defamation and negligence.

Recommendation

4.2 The social and legal issues raised by AIDS should be considered by the relevant professions in the preparation of codes of practice under the data protection legislation (paragraph 4.29).

Historical background

4.3 Before examining the common law remedies with privacy implications, a brief account of the history of a general "tort of privacy" is in order. A "tort" is a civil wrong for which a claim for damages will lie. In a famous Harvard Law Review article in 1906, two American practitioners, Samual Warren and Louis Brandeis, argued that a right to privacy was inherent in the common law. As Wacks puts it:

> *"Drawing upon several decisions of the courts of England, especially in the fields of breach of confidence, copyright and*

defamation, Warren and Brandeis argued that these cases were merely instances and applications of a 'general right to privacy' which was immanent in the common law. They sought to show that the common law had developed from the protection of the physical person and corporeal property to the protection of the individual's 'thoughts emotions and sensations'."[1]

4.4 The author points out that it is debatable whether the authorities Warren and Brandeis cite do strictly support a "right of privacy", particularly *Prince Albert v. Strange*[2]. In that case the plaintiff obtained an injunction restraining the defendant from exhibiting plates of etchings made by Queen Victoria and the plaintiff. The plates had been obtained without their consent. Wacks argues that the actual decision in that case was founded not on the duty of confidence but rather "on a breach by an employee of his duty of good faith to his employer by the disclosure of a trade secret."[3] Fortunately, however, the law is capable of adjusting to changing social conditions and despite these beginnings, by 1960 a tort of privacy had been recognised in 26 States. Of the Commonwealth jurisdictions, New Zealand has been amongst the first to evince support for a tort of privacy. In *Tucker v. News Media Ownership Ltd*[4] the plaintiff required money for an expensive heart operation. A public fund-raising effort was mounted but the defendant received information regarding previous criminal convictions. Fearing publication, the plaintiff sought and obtained an interim injunction restraining the defendant from doing so. However, a radio station then broadcast the information. As the damage was already done the court discharged the injunction, but in so doing McGechan J expressed "support [for] the introduction into the New Zealand common law of a tort covering invasion of personal privacy at least by public disclosure of private facts".

4.5 Recognising that something is desirable is not the same as recognising that it exists. Indeed the words quoted evince the recognition that legal protection was currently lacking. The English Court of Appeal was confronted in stark terms with the issue in *Kaye v. Robertson*[5]. This case concerned a well known television actor who had sustained severe head and brain injuries in a motor vehicle accident. When recuperating in a private room in a hospital a journalist and photographer entered, without hospital permission and contrary to a warning notice on the door. The plaintiff was in no fit state to give his informed consent and did not object to their photographing his pronounced facial scars. Bingham L J described the defendant's conduct as "a monstrous invasion of his privacy" but however gross, that did not entitle the plaintiff to relief under English law. Leggat L J added that the right to privacy had been disregarded for so long in that country that it could be recognised now only by the legislature. He expressed

---

1 Ray Wacks, "The Right to Privacy" in Wacks (ed) *Civil Liberties in Hong Kong* (Oxford University Press, 1988), page 285.

2 (1849) 41 ER 1171.

3 Ray Wacks, *Personal Information*: *Privacy and the Law* (Oxford, Clarendon Press, 1989), pages 82-6.

4 [1986] NZLR 716.

5 [1991] FSR 62 (CA).

the hope that the making good of that "signal shortcoming in our law would not be long delayed".

4.6 There is accordingly no general tort of invasion of privacy in Hong Kong law. The desirability of such a broad remedy will be examined in a subsequent report and it will be seen that other law reform agencies that have examined this proposal have rejected it. A more restricted degree of legal protection is afforded by several common law remedies and in particular the law of contract and breach of confidence. These will now be examined to complete the examination of the protection at present provided by Hong Kong law to information privacy.

The Law of Contract

4.7 The law of contract governs all those agreements between two or more parties where there is an intention to create legal relations supported by mutual promises to give something of value as consideration. Many such contractual relationships involve the disclosure of personal information. Professional relationships are obviously in this category, as well as such relationships as banker and customer, insurer and insured and employer and employed. In all such contracts, it is open to the parties to expressly stipulate terms governing the use and disclosure of personal information which is supplied. Such express terms are relatively uncommon, however, and this is particularly so in relationships such as that of employment where the parties do not possess equal bargaining power. Even in the absence of express agreement, however, the law may imply such a term. The legal basis for implying a contractual term, is that it is founded upon the presumed (as opposed to the express) intention of the parties. It will be seen that it has been held that the contractual relationship of banker and customer contains an implied term that banking records will not be disclosed without authority. This is also the legal position regarding a number of professional and commercial relationships, two of which are discussed below in detail.

4.8 Contract law is inherently limited in its capacity to protect information privacy. A contract is only enforceable against another party to the contract. If that party discloses information to a third party in breach of his contractual obligation, the third party will be unaffected by that obligation. In the absence of a direct contractual relationship, no remedy will lie in respect of his further dissemination of that information unless it is also subject to a common law duty of confidence. That doctrine will now be examined.

Breach of confidence

4.9 Gurry[6] summarises the requirements of this cause of action as follows:

[6] Francis Gurry, *Breach of Confidence,* (Oxford, Clarendon Press, 1984), page 4.

"1. The confider must demonstrate that the information which he has imparted was 'confidential'. As a general rule, confidentiality is established by showing that the information is inaccessible to the public ...

2. The confider must establish that the confidential information was disclosed in circumstances which imposed an obligation on the confidant to respect the confidentiality of the information. Generally, such an obligation will arise whenever information is imparted, either explicitly or implicitly, for a limited purpose. The limited purpose of the disclosure circumscribes the nature of the confidence between the parties by imposing on the confidant a duty to refrain from using the information for any extraneous purpose. The obligation of confidence thus formed extends not only to those confidants who have received confidential information for a limited purpose, but also to any third parties to whom the confidant discloses the information in breach of his obligation.

3. Having established that confidential information has been disclosed in circumstances which impose an obligation of confidence on the confidant, the confider must finally show cause for invoking the aid of the courts to enforce the confidence. He must show that the confidant has breached the obligation. This requirement is satisfied when it is shown that the confidant has made an unauthorised use of the information by using it for a purpose other than that for which it was imparted to him."

Confidentiality and the Use Limitation Principle

4.10 It will be recalled from Chapter 2 that the OECD data protection guidelines include the Purpose Specification Principle and Use Limitation Principles, the thrust of which is that information should be used only in accordance with the purpose for which it was provided. The affinity with the duty of confidence set out above will be apparent.

Limitations of the duty of confidence in protecting privacy

4.11 As compared with the data protection principles, the legal duty of confidence affords only limited protection to information privacy. The principles encompass such varied matters as fair obtaining, limits on disclosure, access and correction rights, and data security. The legal duty of confidence restricts its attention to limited disclosure. Even as regards this aspect of information privacy, the duty has a narrower scope of application than the Use Limitation Principle. Only the person who imparts the information is owed the duty of confidence and is accordingly entitled to enforce it. Therefore, where an employer provides in confidence an

employment agency with information concerning but not obtained from a former employee, only the employer and not the employee would have a legal remedy against the employment agency for a breach of that confidence. This is attributable to the legal policy interests the duty seeks to protect:

> *"The purpose of the law of confidence, on the other hand, though it requires the information to be 'confidential', is essentially to maintain the fidelity or trust that the plaintiff has reposed in the person to whom he has confided (or, at any rate, who ought to recognise that he is breaching such trust). The policy of the law is essentially to promote the honesty (or, at any rate, absence of deception) which is an important aspect of commercial transactions."*[7]

4.12 By comparison, the Use Limitation Principle does not concern itself with the source of the disclosure, so that in the example above the former employee would be entitled to complain if the agency disclosed the information for a purpose other than that for which the employer provided it.

4.13 As well as being narrower in scope than a protection of personal information as such, the remedy the cause of action affords is of less utility where personal information is involved than it is for the trade secrets that have comprised the action's staple diet to date. This is because a person will be disinclined to air his private life in a court action. This is quite apart from the general disincentives facing all litigants, namely the expense of court proceedings and the uncertainty of their outcome. The uncertainty aspect is exacerbated in breach of confidence actions because a specific defence available is that the unauthorised disclosure is in the public interest. This defence involves the court in the necessarily imprecise exercise of weighing the public interest in maintaining confidentiality against the public interest in its disclosure. An additional source of uncertainty derives from the defence that the confider consented to the disclosure expressly or impliedly. This is a question of fact upon which judicial minds will doubtless differ and it will be seen below a UK committee has recently recommended that the defence be abolished in the banking sector.

The media and privacy

4.14 It is presumably for reasons such as those outlined above that a recent review of the English case law concluded that "authority is scant on the extent to which personal confidences may be the subject matter of a legal obligation of confidentiality."[8] An area, however, where the action has been employed comparatively frequently is where the media has publicised or proposed publicising private matters. This is a complex area which we partially address in Chapter 18. It may, however, be useful to point out that,

---

7 Wacks, *op cit*, page 127.

8 William Wilson, “Privacy, Confidence, and Press Freedom: A Study in Judicial Activism" (1990) *53 Modern Law Review*, page 43.

though in a number of cases[9] the courts have been required to apply the action in circumstances where "personal information" has been disclosed (by the press) this has not been a particularly satisfactory exercise and several difficulties have arisen. For example, the general requirement that there must be a relationship between the person who confides the information and the person to whom it has been confided (see below, para 4.15) means that where a newspaper has obtained the information *without* a breach of confidence, it may not be subject to the court's jurisdiction. Similarly, the requirement that the plaintiff must establish that the information was not in the public domain, produces artificial results in cases involving "personal information". In general, the action for breach of confidence is an inadequate means by which to protect individuals against publicity being given to private facts, for the action is primarily concerned with:

(a) *disclosure* rather than *publicity*;

(b) the *source* rather than the *nature* of the information;

(c) the *preservation of confidence* rather than the possible *harm* to the plaintiff. [10]

These, and other, difficulties are dealt with separately when we come to consider the question of privacy and the media.

Relationships and the duty of confidence

4.15 Before examining the duty of confidence as it arises in the course of particular relationships, the question requires addressing whether the protection afforded by the action is restricted to such relationships, or whether it arises solely from the disclosure of confidential information. Does the disclosure of personal information outside the context of an extraneously established relationship of trust attract a duty of confidence? A recent analysis[11] suggests that there has been a significant shift of judicial emphasis. Prior to 1988 the cases were equivocal on this point but in *Stephens v. Avery* it was held that it is not necessary for a recognised relationship to predate the protected disclosure:

> *"The basis of equitable intervention to protect confidentiality is that it is unconscionable for a person who has received information on the basis that it is confidential subsequently to reveal that information. Although the relationship between the parties is often important in cases where it is said there is an implied as opposed to express obligation of confidence, the relationship between the parties is not the determining factor. It*

---

9 See, for example, *Argyll v Argyll* [1967] Ch. 302; *Woodward v Hutchins* [1977] 1 WLR 760; *Lennon v News Group Newspaper Ltd* [1978] FSR 573 and *Khashoggi v Smith* (1989) NLJ 168.

10 See Wacks, *op cit,* page 134. The inadequacy of the law is examined by Sir David Calcutt (Home Office, *Report on the Committee on Privacy and Related Matters*, Cmnd 1102, 1990.

11 Wilson, *op cit,* see note 5.

is the acceptance of the information on the basis that it will be kept secret that affects the conscience of the recipient of the information."[12]

4.16 In that case the plaintiff had imparted to the defendant information relating to her sexual activities expressly on the basis that it must not be repeated. Instead, the recipient disclosed this information to the press. The plaintiff and defendant were not in a pre-existing relationship such as marriage or a professional relationship. They were simply friends. It was held that a duty of confidence arose nonetheless where the disclosure was made on the express basis that it was to go no further. It has been pointed out[13] "that despite his statement that 'the relationship between the parties is not the determining factor', the Vice-Chancellor was obliged to emphasise the fact that 'the express statement that the information is confidential is the clearest possible example of the imposition of a duty of confidence.'" However in the recent Hong Kong Supreme Court decision of *Koo and Chiu v. Hing*[14] (upheld on appeal) Bokhary J held that there had been a breach of confidence not only where the parties were not in a relationship, but also where the plaintiffs had not entrusted the information to the defendant. It was held sufficient that the defendant had obtained the information in circumstances indicating that it was not available for him to use. The information held to be confidential in that case was not personal information, but questionnaires.

Contract and the duty of confidence

4.17 Notwithstanding these developments, the courts are more disposed to accord protection to information disclosed in the course of certain relationships which it recognises as intrinsically confidential. These relationships are often also contractual in nature and it may also be a condition of the contract that information not be disclosed without authority. The protection afforded by contract and the duty of confidence operate independently:

"The law has long recognised that an obligation of confidence can arise out of particular relationships. Examples are the relationships of doctor and patient, priest and penitent, solicitor and client, banker and customer. The obligation may be imposed by an express or implied term in a contract but it may exist independently of any contract on the basis of an independent equitable principle of confidence."[15]

4.18 In view of their independent operation the obligations may co-exist in some relationships. They are not necessarily co-extensive, however. The obligation not to disclose confidential information may differ in content from the contractual term, as a result of the former's requirement that the

---

12 [1988] 2 All ER 477, at 482.

13 Wacks, *op cit*, see note 2.

14 [1992] 2 HKLR 314, and unreported 1992, No. 116 (Civil).

15 per Lord Keith in *A-G v. Guardian Newspapers* (No 2) [1988] 3 WLR 776, at page 781.

information disclosed is indeed "confidential" and not public knowledge. The contractual duty, on the other hand, may extend to all information acquired during the course of the contract.

Bankers and doctors: examples of contractual/confidential relationships

4.19 The existence of a legal remedy can beneficially influence standards of conduct even if seldom invoked in practice, provided those potentially affected are aware of it. This situation obtains in a number of recognised relationships, particularly professional relationships. The following is a brief description of two of the more important relationships where an obligation of secrecy arises from contractual and/or equitable principles. The relationships chosen for description (the banking and medical relationships) highlight areas of rapid social and technological change. Not surprisingly, they reveal the difficulty the traditional duty of confidence has coping with an increasingly complex world. But such complexity argues against the adequacy of *any* very general legal framework in the absence of supplementary provisions attending to the sectoral problems involved. This fundamental point is relevant to our main recommendation below that Hong Kong enact a data protection law. We also recommend below that such a law should be supplemented by sectoral codes to accommodate the sort of specific problems arising in the following areas.

Banker and Customer

4.20 The leading decision on the banker's obligation of secrecy is the English Court of Appeal decision of *Tournier v. National Provincial and Union Bank of England*[16]. The headnote of the decision states:

> *"It is an implied term of the contract between a banker and his customer that the banker will not divulge to third persons, without the consent of the customer express or implied, either the state of the customer's account, or any of his transactions with the bank, or any information relating to the customer acquired through the keeping of his account, unless the banker is compelled to do so by order of a court, or the circumstances give rise to a public duty of disclosure, or the protection of the banker's own interests require it."*

4.21 It appears that the contractual obligation of a bank limiting disclosure extends to publicly available information it holds on a customer[17]. In addition to this obligation of secrecy arising from contract, there is also the duty of confidence which would arise, for example, when potential banking

---

16 [1924] 2 KB 461.

17 G. Burton and P. Jamieson, "Modern Banking Services: Rights and Liabilities" (1989) *63 Australian Law Journal*, page 595.

customers disclose confidential information prior to entering a contractual relationship.[18]

4.22 While these broad principles are settled enough, much of the present scope of a banker's duty of confidentiality is uncertain. Uncertainty has even been discerned on the fundamental point of whether it extends to bankcard operations[19], although in principle it should. The uncertainties have been identified and addressed in a comprehensive 1989 UK report of the Review Committee chaired by Professor R B Jack.[20] It notes the impact of ever-accelerating electronic banking and the increasing legislative abrogation of banking secrecy to combat crime. It concludes that although the principle enunciated in *Tournier* remains valid, its exceptions are not closely defined enough for today's conditions. It recommends a statutory codification of a modified version of the *Tournier* rules. Those modifications would include:

(a) abolition of a general exception of a duty to the public to disclose, in view of the proliferation of specific provisions to this effect;

(b) closely defining the specific situations where the interests of the bank require disclosure;

(c) restriction of the exception of disclosure with the customer's consent to express written consent. The present exception of implied consent would be abolished in view of its uncertain application and the concern that business competition could tempt banks to overly rely on it instead of seeking confirmation from the customer. The requirement of express consent would include disclosure to credit reference agencies of "white" credit information (ie regarding customers not in default).

(d) that the well established practice whereby banks respond to inquiries or references on customers (known as banker's opinions, bankers' references or status enquiries) is widely misunderstood and even mistrusted by the customers this non-profit-making service is presumably intended to assist. The banks have traditionally invoked the implied consent justification. To combat misunderstanding, customers should have the system explained to them when they open an account and be invited to give or withhold their consent.

4.23 Following the Jack Committee's report and the Government response to this, a voluntary Code ("Good Banking") was drawn up by the British Bankers' Association, the Building Societies' Association and the Association for Payment Clearing Services. This Code, which came into

---

18 J. Walter and N. Erlich, "Confidence: Bankers and Customers" (1989) *63 Australian Law Journal,* page 404.

19 Australian Law Reform Commission, *Privacy* (Report No. 22), Canberra: 1983, page 193.

20 *Banking Services,* Cmnd 622.

effect on 16th March 1992, addresses the question of confidentiality of customer information in the following provision:

> *"CONFIDENTIALITY OF CUSTOMER INFORMATION*
>
> *6.1 Banks and building societies will observe a strict duty of confidentiality about their customers' (and former customers') personal financial affairs and will not disclose details of customers' accounts or their names and addresses to any third party, including other companies in the same group, other than in the four exceptional cases permitted by the law, namely:*
>
> *(i) where a bank or building society is legally compelled to do so;*
>
> *(ii) where there is a duty to the public to disclose;*
>
> *(iii) where the interests of a bank or building society require disclosure;*
>
> *(iv) where disclosure is made at the request; or with the consent, of the customer.*
>
> *6.2 Banks and building societies will not use exception (iii) above to justify the disclosure for marketing purposes of details of customers' accounts or their names and addresses to any third party, including other companies within the same group.*
>
> *6.3 Banks and building societies will at all times comply with the Data Protection Act when obtaining and processing customers' data.*
>
> *Banks and building societies will explain to their customers that customers have the right of access, under the Data Protection Act 1984, to their personal records held on computer files."*

4.24 In Australia the legal uncertainties described coupled with lack of customer awareness of their bank's practices (both generally and as regards specific transactions) "produced a situation where practices although of doubtful legal validity have become standard".[21] These factors are also presently at work in Hong Kong. (One of the few commentaries on the local situation is found in the *South China Morning Post* of 2 December 1986 which canvasses a number of conflicting views by local bankers on the extent to which the banks here uphold the confidentiality of their customer's affairs. The same paper's 7 February 1991 issue reported that a computerised

[21] Australian Law Reform Commission, *op cit*, see note 12, page 402.

blacklist of shops suspected of involvement in credit card fraud would be on-line to banks and credit card companies from April. Apparently those blacklisted were not to be advised). The implementation of the Jack Committee's recommendations in Hong Kong would help redress the recent erosion of the banker's obligation of secrecy. As an international financial centre, Hong Kong should be astute to maintain high standards in this aspect of customer service. It is worth noting that the UK banking code supplements the protection already afforded by the United Kingdom Data Protection Act.

Medical practitioner and patient

4.25 Where there is a contract between a doctor and a patient, involving the provision of professional services in return for a fee, it is an implied term of that contract that the doctor will maintain confidentiality as regards the patient's medical condition. The modem provision of medical services will often result, however, in there being no contractual relationship between the doctor and patient, eg where salaried doctors are employed by public hospitals. In such cases the patient can look to protection from the duty of confidentiality which encompasses not only information imparted by the patient but also that derived from the doctor's physical examinations and testing, as well that provided by consultants' reports.[22]

4.26 The provision of medical services has become increasingly sophisticated and the following areas deserve discussion:

(1) **The employee doctor.** This aspect was clarified in *Slater v. Bissett*[23]. There the doctor was a salaried doctor employed by a health authority which introduced measures which he legally challenged as tending to interfere with his duty of confidentiality. The court held that a patient consulting an Authority doctor "is to be taken as accepting impliedly the administrative procedures which are adopted by that authority". So where the patient records are kept by a central office registry, the patient (who has no ownership of the records simply because he generates them) can be taken to impliedly consent to the authority's staff seeing those records "at least in passing". In the hospital setting, the implied consent would extend to disclosure to all the health professionals, ranging from radiologists to dieticians involved in a patient's treatment. They too would be subject to the duty of confidence as regards the information entrusted to them. *Slater* makes it clear that this duty cannot be overridden merely on the instructions of the confidant's superior officer.

(2) **Doctor engaged to repo**rt **to an institution.** It commonly occurs that a person is required to undergo a medical examination to obtain insurance or employment. The examining doctor will nonetheless owe a duty to the examinee not to

22 *ibid,* at page 415.

23 (1986) FLR 118.

communicate the information except to the extent necessary to discharge the reporting function. Similarly, the institution acquiring the report will be legally bound to disclose it only to the extent necessary to fulfil the purpose of the examination.

(3) **Human medical research.** The legal principle of confidentiality of medical information arguably precludes the lawful use of medical records relating to identifiable subjects for the purposes of medical research. The social utility of such research is evident but is not accommodated by the legal duty of confidentiality discussed above. Whilst that principle recognises the defence of disclosure "in the public interest", in the absence of clear authority on the point it is unclear whether this extends to disclosure for research purposes. The problem is considered in the 1990 report of the Law Reform Commission of Western Australia on *Confidentiality of Medical Records and Medical Research* which recommends the enactment of legislation to permit this. This would accommodate epidemiological research involving often large samples, much of which would be severely inhibited by restrictions on the use of name-identified patient information in the absence of patient consent. To date Hong Kong also lacks legislation addressing the issue of medical research, but we address the issue in Chapter 15.

AIDS and privacy

4.27 AIDS was the subject of a breach of confidence action in *X v. Y* [1988] 2 All ER 648. In that case information was leaked to a newspaper by employees of a health authority disclosing the identity of two doctors suffering from AIDS. The health authority sought to restrain the publication of this information and the court so ordered. It held the public interest in preserving the confidentiality of hospital records identifying AIDS sufferers outweighed the public interest in the freedom of the press to publish such information. This was because victims of the disease ought not to be deterred by fear of discovery from going to hospital for treatment, and free and informed public debate could take place without publication of the confidential information acquired by the defendants. The decision does not specifically relate to the confidential relationship of doctor and patient. Its significance resides, however, in the importance the court attached to the public interest in preserving the confidentiality of the identity of AIDS patients and this would be relevant to the extent of a doctor's duty of confidentiality when confronted by competing legal duties, such as the duty of care in negligence to inform partners potentially at risk (this has been legislated on in California in favour of the latter[24]).

[24] See D and S Pearl, "Aids: An Overview of the Legal Implications" (1989) 19 *Law Society's Gazette*, page 28.

4.28 AIDS raises difficult issues which have recently been to the fore locally. The following issues have received local press attention:

(a) Whether the Hong Kong health authorities should issue medical certificates to those of its residents seeking to work in China.[25]

(b) Evidence that leading Hong Kong companies are ignoring World Health Organisation guidelines by testing potential employees for the HIV virus.[26]

(c) Whether there should be legislation requiring HIV positive adults to notify their sexual partners. A Health spokesman has expressed scepticism about the proposal as it could deter people from coming forward for testing.[27] A related problem arises when a doctor can reasonably foresee that a spouse or other third party may be infected unless he informs them of his patient's infection. He is then confronted with a conflict between his duty of confidence and an arguable duty of care in negligence. The United Kingdom Medical Defence Union has advised its members to defer to the latter.[28] Hong Kong doctors lack legal guidance on this increasingly common question.

(d) Evidence that most local life insurance companies arrange HIV testing for high level cover without obtaining express consent or advising of the result. In one instance an applicant was rejected on the given ground of a "major problem". It took him three weeks of correspondence to ascertain that he had been tested as HIV positive. The insurer had by this time disclosed the result to a third party. Subsequent testing showed that the initial positive diagnosis was false.[29]

4.29 These issues go beyond the scope of our terms of reference, insofar as confidentiality is only one aspect. The present legal framework does appear inadequate, however, and **we recommend that it be specifically considered by the relevant professions in the preparation of codes of practice under the data protection legislation.**

Disclosure of confidential information in litigation

Public interest immunity

4.30 We have seen that the equitable principle of confidentiality affords protection against the disclosure of information which has been entrusted in circumstances imposing on the recipient an obligation not to

---

25 *Hong Kong Standard*, 30 December 1989.
26 *South China Morning Post*, 30 December 1992.
27 *Hong Kong Standard*, 23 March 1991.
28 Pearl, *supra*.
29 *South China Morning Post*, 27 and 28 August 1991.

disclose such information without consent. Confidentiality may arise from and attach to a communication where the parties are not in a confidential relationship as such. Alternatively the parties may be in a relationship which the law recognises as confidential and the obligation of confidence will attach to communications made in the course of that relationship. Some of the cases discussed above deal with the question of whether communications which it is conceded *are* confidential should be disclosed in the course of court proceedings. This raises the applicability of the legal principle known as "Public Interest Immunity", under which evidence which is relevant and admissible under the ordinary rules of evidence will be excluded if the court is of the opinion that its disclosure is contrary to the public interest. This doctrine used to be known as "Crown Privilege" but it is now clear that any party may apply under this principle to have evidence excluded.

4.31 In determining whether to exclude evidence on the basis of this principle, the court has to weigh the potential harm to the community if the evidence is admitted against the need to have before it all the relevant evidence necessary to fairly determine the case. Where the evidence pertains to such matters as national security and the identity of police informers, the court will be disposed to exclude the evidence. In *Campbell v. Tameside MBC* Ackner LJ put it in the following terms:

> *"The fact that information has been communicated by one person to another in confidence is not, of itself, a sufficient ground for protection from disclosure in a court of law of either the nature of the information or the identity of the informant if either of these matters would assist the court to ascertain facts which are relevant to an issue on which it is adjudicating: see Alfred Compton Amusement Machines Ltd v. Customs and Excise Comp (No 21) [1974] AC 405. The private promise of confidentiality must yield to the general public interest, that in the administration of justice truth will out, unless by reason of the character of the information or the relationship of the recipient of the information to the informant a more important public interest is served by protecting the information or identity of the informant from disclosure in a court of law: see D v. National Society for the Prevention of Cruelty to Children [1978] AC 171. Immunity from disclosure was permitted in that case because the House of Lords recognised the special position of the NSPCC ... a position which the House saw as comparable with that of a prosecuting authority in criminal proceedings. It applied the rationale of the rule as it applies to police informers, that if their identity was liable to be disclosed in a court of law, this source of information would dry up and the police would be hindered in their duty of detecting and preventing crime."*[30]

[30] [1982] 2 All ER 791, at 796.

Professional privilege

4.32 The immunity described above based upon the public interest cannot be waived by the parties and will be invoked by the court even if not raised by the parties. The principle differs in this respect from legal professional privilege. That is the principle whereby a solicitor must not produce or disclose in any legal proceedings any communication between himself and his client without the client's consent. It is distinct from and additional to the more general equitable duty of confidence which applies generally to professional relationships. That more general duty does not extend to court proceedings. Nor does professional privilege apply to professions other than lawyers, such as clergymen, bankers, doctors or journalists. This was established in *British Steel v. Granada Television*[31] where journalists unsuccessfully sought to invoke an immunity analogous to legal professional privilege protecting them from the obligation to disclose in a court of law their sources of information, such disclosure being necessary in the interests of justice. We note that the right to confidential legal advice is provided for in article 35 of the Basic Law.

Confidentiality and copyright compared

4.33 Copyright is a proprietary right relating to tangible works such as literary and scientific texts and artistic objects. It is protected by legislation rather than common law. *Fraser v. Thames Television*[32] usefully highlights the difference between copyright and the duty of confidence. That was a breach of confidence action in respect of disclosure of a dramatic idea which ultimately found expression in the "Rock Follies" television series. Counsel for Thames Television argued that since an idea is not protected by copyright, then by analogy it was not protected by breach of confidence. Hirst J said, however, that:

> *"I do not find the argument by analogy with copyright cases helpful. The law of copyright is about copying. It is of the very essence of copyright that it protects material in permanent form ... On the other hand, under the general law of confidence the confidential communication relied on may be either written or oral ... Copyright is against the world generally, whereas confidence only protects against those who receive information or ideas in confidence. Although copyright has a fixed (albeit extensive) statutory time limit, and confidence, at all events in theory, no time limit, in practice the obligation of confidence ceases the moment information or idea becomes public knowledge. Furthermore, although the law of copyright protects unpublished as well as published works, it is no part of its purpose to protect confidentiality as such. Indeed section 46(4) of the 1956 Act [applying to HK] expressly provides that 'nothing*

31 [1981] AC 1096.
32 [1983] 2 All ER 101.

in this Act shall affect the operation of any rule of equity relating to breaches of ... confidence'."[33]

Privacy and copyright

4.34 Under the existing Hong Kong copyright regime which applies the repealed United Kingdom Copyright Act 1956, it can be argued that a right of privacy is recognised in relation to the commissioning of the making of a portrait or engraving or the taking of a photograph since the incidence of ownership rests with the commissioning party unless there is an agreement to the contrary.

4.35 The United Kingdom copyright regime makes special mention of copyright and privacy. Section 85 of the Copyright, Designs and Patents Act 1988 provides, among other things, the right of privacy of certain photographs and films. A person who for private purposes commissions the taking of a photograph or the making of a film, where copyright subsists in the resulting work, has certain rights not to have copies of the work issued to the public or the work exhibited or show in public or broadcast.

4.36 It is likely that Hong Kong will follow this provision of the 1988 Act by vesting the copyright to the maker of such a work. It appears that there is a need to allow the commissioning party to restrain unauthorised use of the work which may affect his privacy.

Defamation

4.37 Apart from breach of confidence, the only action under common law which offers any significant incidental protection to information privacy is that of defamation. A defamatory statement has been succinctly defined by Louis Blom-Cooper QC as "the publication (including orally) to a third person of matter which in all the circumstances would be likely to affect a person adversely in the estimation of reasonable people generally". The principal limitation of the action as regards information privacy, however, is that it is a total defence that the statement is true, regardless of the motive in disparaging the person whose reputation is thereby damaged. Obviously a person's privacy might be infringed by a statement which is true. As Warren and Brandeis pointed out, in most circumstances where publicity is given to a person's private life, the person's interest is not merely "to prevent inaccurate portrayal of his private life, but to prevent its being depicted at all".

4.38 In view of the above, it has been argued by the Faulks Committee on Defamation that the "concepts of defamation and intrusion into privacy should be kept distinct from one another". They are assimilated to an extent, however, in those legal systems which provide that a defence of justification or truth should not succeed unless the defendant proved not only

---

[33] *ibid*, at 117.

that the words were true but also that there was a legitimate interest of the public in being informed about the subject matter published. The question of the media and data protection is examined in Chapter 18. In the present context, however, it suffices to note that at present Hong Kong defamation law affords very limited protection to information privacy.

Negligence

4.39 Negligence is a cause of action affording redress in respect of a breach of a standard of care owed to the plaintiff and resulting in a reasonably proximate material injury to his interests. Additionally there are circumstances in which there is a duty to take reasonable care not to make false statements which cause the recipient economic loss. This includes the negligent provision of false information and in unusual circumstances an omission to inform a person of a relevant fact.

4.40 In order to establish this duty it is normally necessary to prove:

(a) that a commercial transaction or purpose is concerned;

(b) that the informant intended the statement to be relied upon for that transaction or purpose from the nature and gravity of the enquiry;

(c) that the recipient actually and reasonably relied upon the statement;

(d) that economic loss of the kind suffered was foreseeable; and

(e) that the parties were sufficiently "proximate".

4.41 An informant may also be liable to those who do not request the information themselves if it is provided or volunteered to a recipient not only as an individual but as a member of an identifiable class in respect of a transaction of a specific kind.

4.42 This branch of the law does not protect the privacy of personal information. In rare cases it provides a sanction which encourages an informant to be careful about the accuracy of any information which he imparts whether or not it is personal. For practical purposes it is irrelevant to this reference and does not merit more detailed consideration.

Chapter 5

The protection of personal data in Hong Kong - the need for reform

Summary

5.1 This chapter sets out the reasons why we consider it essential that the international standards of privacy protection contained in the internationally agreed data protection principles and the privacy provision of the ICCPR be incorporated into Hong Kong's domestic law. The chapter highlights the pressing international trade considerations which argue for early recognition of these standards.

5.2 We examine the extent to which the international standards are recognised in the existing law in Hong Kong and conclude that existing statutory protection of information privacy is scattered and incidental in nature. Article 14 of the Bill of Rights Ordinance provides some broad protection against public sector intrusion on privacy, but not against infringements by the private sector.

5.3 The limited remedy provided by breach of confidence is the only common law doctrine which is specifically directed at restricting the disclosure of personal information.

5.4 We examine the feasibility of continuing to rely on the existing voluntary controls and conclude, in the light of experience elsewhere, that statutory intervention is now required.

Recommendation

5.5 The internationally agreed data protection guidelines should be given statutory force in both the public and private sectors. (paragraph 5.43)

International impetus for data protection

5.6 In Chapter 2 we discussed the international developments providing the impetus for an increasing number of countries enacting legislation protecting personal data. There are two main aspects: international trade in personal information and human rights treaty obligations.

International trade in personal information

5.7 If Hong Kong is to retain its status as an international trading centre, it is vital that it participates in the burgeoning international exchange of personal data. Increasingly, its capacity to do so will depend on its satisfying other countries that it offers an adequate level of legal recognition of the data protection principles. A growing number of countries have included in their laws protecting personal data provisions empowering the data protection authority to prohibit export when it is not satisfied with the importing country's level of protection. Specific instances were given in Chapter 2. In one case, the French authority required a contract to be entered into. In the other, the United Kingdom authority banned the export of data to the United States. Hong Kong will remain vulnerable to such measures until it enacts adequate statutory protection. The draft Directive of the Commission of the European Communities requires all Member States to make provision in this regard. The Commission anticipates that the Directive may be adopted in 1994 and implemented in mid 1996. It is also noteworthy that article XIV of the recently concluded General Agreement on Trade and Services specifically allows for measures relating to the protection of privacy in relation to personal data. At a more subtle and pervasive level, responsible overseas companies will be inhibited from exporting personal data to Hong Kong.

Human Rights treaty obligations to protect privacy

5.8 Article 17 of the ICCPR provides for a guarantee against arbitrary or unlawful interference with privacy. The Human Rights Committee's general comment has more fully articulated the application of that provision to information privacy, although it is less comprehensive than the internationally agreed data protection principles. It provides in part that:

> *"The gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law."*

5.9 The ICCPR requires State Parties to submit regular reports to the Human Rights Committee on the measures they have taken to give effect to the guaranteed rights. The third such report on Hong Kong (1991) refers to the Law Reform Commission being tasked to formulate proposals on the matter.

5.10 The enactment in 1991 of the BOR has effected the incorporation of article 17 into Hong Kong's domestic law, as article 14 of the Ordinance, but it binds only the government and public authorities. It provides no protection to the individual where his privacy is interfered with by another individual or a private body. In this respect, the treaty requirements have yet to be given statutory recognition in Hong Kong.

Present domestic legal status of international privacy norms

5.11 The previous chapters have examined the existing legal framework and it is now necessary to scrutinise the extent to which that framework affords protection to information privacy in the light of the requirements of article 17 of the ICCPR and the internationally agreed data protection principles.

Present level of legal recognition of data protection principles

5.12 What follows is a review of the extent to which the international standards of information privacy are currently incorporated in Hong Kong's domestic law. The discussion focuses on the international data protection principles as the relevant standards. They are more comprehensive than article 17 and accordingly encompass that provision's requirements concerning information privacy. It is their legal recognition which will determine Hong Kong's prospects of fully participating in the international trade in personal data. For the purposes of exposition, the OECD Guidelines are referred to, but as indicated earlier these cover much the same ground as the other formulations of the Council of Europe and the Commission of the European Communities. Also, we have differentiated the different stages of data processing for the purposes of analysis, although the OECD cautions that:

> *"The distinction between different activities and stages involved in the processing of data which are assumed in the principles, are somewhat artificial and it is essential that the principles are treated together and studied as a whole."*[1]

Collection

5.13 The information processing cycle begins with the collection of information. The OECD Collection Limitation Principle provides for this stage as follows:

> *"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 or consent of the data subject."*

5.14 This principle emphasises that the collection of information should be by fair and lawful means. In this context "lawful" would encompass both common law and statutory requirements. The collection of information entailing a breach of either contract or the duty of confidence is already unlawful, and repetition of the lawfulness requirement in the principle means

---

1 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris: OECD, 1981, paragraph 50.

that it would contravene that also. The ambit of "fair" is less clear. Those means which constitute flagrantly intrusive conduct (such as telephone tapping) will be examined in a subsequent report. But "unfair" collection would include subtly coercive or deceptive practices. Coercion or deception may reach the point of being tortious or criminal but at present there are no legal norms, statutory or common law, providing a positive requirement of fair collection. To anticipate the discussion in Chapter 9, "fair" collection requires the knowledge and preferably the consent of the data subject.

5.15 Information should not be collected unnecessarily. The Data Quality Principle requires that "personal data should be relevant to the purposes for which they are to be used". The data subject may have some say in this. His provision of the information may be voluntary in the sense that, although provided in response to a request, there is no legal compulsion, nor is there the prospect of being denied a benefit. In these circumstances the data subject can restrict the information he provides to that which appears relevant. But often disclosure will not be voluntary. In Chapter 3 we examined a number of ordinances which impose statutory requirements that personal information be furnished. The ordinances differ in the extent to which the information required is apparently relevant to the statutory functions in question. When the legislation does not in terms delimit relevant information requiring disclosure, irrelevant information may be requested by officers clothed by the mantle of apparent authority.

5.16 Even in the absence of a statutory provision compelling disclosure, the imparting of information may not be truly voluntary, in that it may be necessary to obtain a benefit. A public sector example is applying for a licence. A private sector example is a loan application. While legislation may define with some particularity the information required by applicants to obtain a benefit or avoid a detriment being imposed by the public sector, there are no statutory or common law controls limiting the ambit of personal information that may be required by the private sector. It is entirely at the discretion of the person making inquiries whether he restricts his questions to reasonably relevant matters.

5.17 The OECD Data Quality principle, it will be recalled, requires that to the extent necessary for the purposes for which data are to be used, they "should be accurate, complete and kept up-to-date." In Chapter 1 (paragraph 1.10) we looked at studies indicating that inaccuracy of records is a major problem. The law of negligence may sometimes provide a remedy, but this would only extend to foreseeable harm. Given the ease of modem technology in rapidly and widely disseminating information, this may be impossible to establish.

5.18 The reliability of information generally deteriorates with age. The answer is regular purging, but computerised systems lack the same incentives of pressure of space and storage costs which encourage the culling of manual records. Computerisation also facilitates the sharing of information by a number of entities and even the remote possibility that the information may someday be sought by one of them may also inhibit purging. For these

reasons a computer's capacity to be readily programmed to remove obsolete material may not be invoked, frustrating the "right to be forgotten". Archival material is an exception to the generalisation that the value of material deteriorates with age. The special position of both manual and computerised archival material requires separate consideration.

5.19 Many records contain inaccuracies which are never remedied because the data subject is never acquainted with them. Access to records facilitates their correction. The Openness Principle and the Individual Participation Principle address this and are dealt with below.

Disclosure

5.20 The use and disclosure of personal information is central to the information processing cycle. The two relevant OECD principles are the Purpose Specification Principle and the Use Limitation Principle. The former provides that "the purposes for which the personal data are collected be specified not later than at the time of data collection" and that "the subsequent use be 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 of purpose". The Use Limitation Principle provides that "personal data should not be disclosed, made available or otherwise used for purposes other than those" in accordance with the Purpose Specification Principle. The only exceptions are where the disclosure occurs with the consent of the data subject or pursuant to legal authority.

5.21 Hong Kong currently possesses only limited legal controls to ensure the observance of these two principles. For convenience the following summary deals separately with the public and private sectors, but it should be noted that the application of the distinction is not always clear with autonomous public bodies such as the Mass Transit Railway Corporation. This is but one of the reasons why we recommend below that both sectors should be subject to the same data protection controls.

Public sector

5.22 In Chapter 3 we looked at the statutory constraints on government departments using and disclosing information for purposes different from those for which it was initially obtained. We saw that comparatively few ordinances contain secrecy provisions, the legislative method of restricting disclosure to other departments and the public. Even secrecy provisions are generally couched in terms which sanction disclosure occurring in the performance of the officer's duties. However, the majority of ordinances which provide for the compilation of personal records lack secrecy provisions in any event. On the other hand, they also generally lack statutory provisions authorising the disclosure of information to other authorities.

5.23 The duty of confidence may attach to information furnished on a voluntary basis to a public authority. We have seen, however, that in the case of *Hall v. ICAC*[2], the Hong Kong Court of Appeal did not envisage that duty arising when the information was obtained under compulsory powers. The decision could be interpreted as sanctioning the exchange by public authorities of personal information compulsorily obtained, in the absence of express statutory provisions authorising such disclosure, provided it is not prohibited by a secrecy provision. The subsequent English Court of Appeal decision to the contrary of *Marcel v. Commissioner of Police*[3] adopts a narrower view. That held that the information is subject to a duty of confidence and a public authority will only be authorised to disclose such information for a purpose envisaged by the statute authorising its collection. *Marcel* accords with the BOR, whereas *Hall* does not, particularly as regards automated data (which is the particular focus of the Human Rights Committee's general comment).

Private sector

5.24 The legal duty of confidence has a less problematic application in the private sector than presently obtains in the public sector. We have seen that there is an affinity between the duty of confidence (and/or the implied contractual duty of confidence) and the combined operation of the Purpose Specification Principle and the Use Limitation Principle. In addition, the key relationships which are especially likely to elicit sensitive information are often also contractual in nature. The implied contractual duty of confidence and the equitable principle supplement each other's operation in this context. In so doing, they provide a degree of legal support for the Use Limitation Principle and the Purpose Specification Principle. We examined for illustrative purposes two confidential relationships, namely banker/customer and doctor/patient, and saw that technological and social changes were outstripping the capacity of these traditional common law remedies to provide protection which was sufficiently certain in scope.

5.25 Whilst contractual undertakings of secrecy and the duty of confidence cover some of the same ground as the Use Limitation and Purpose Limitation Principles, the latter have a much broader role than the common law principles in the protection of information privacy. Only some relationships are contractual and only the parties to the contract may enforce it, whereas the information may pertain to third persons. Similarly, the legal duty of confidence may only be enforced by the confider, and even then he must incur the significant costs, uncertainty and delays inherent in any litigation. As well as being subject to these practical objections, it is also unsatisfactory in principle, because at the heart of information privacy is the notion that it is the person to whom the information pertains who should have a degree of control over its use. The data protection principle limiting the use of personal data to its specified purpose is not subject to the inherent

---

2 *op cit.*

3 *op cit.*

limitation that only the confider may enforce it, as the data subject may also do so.

5.26 In one major respect, the private sector affords less privacy protection to individuals than does the public sector. The BOR, including its privacy provision, only binds the public sector. It provides no protection where the intrusion is by another individual. Section 7 of the BOR provides:

> *"(1) This Ordinance binds only-*
>
> *(a) the Government and all public authorities; and*
>
> *(b) any person acting on behalf of the Government or a public authority."*

5.27 This provision was considered by the Court of Appeal in *Tam Hing-yee v. Wu Tai-wai*[4]. The facts of that case were that a judgment creditor had secured a court order prohibiting the respondent from leaving Hong Kong. The court at first instance held that the legislative provision pursuant to which the prohibition order was made was contrary to article 8 of the BOR. That provides for liberty of movement, including the right to leave Hong Kong. The court accordingly further held that article 8 stood repealed by reason of article 3 which provided that:

> *"all pre-existing legislation that does not admit of a construction consistent with this Ordinance is, to the extent of the inconsistency, repealed."*

5.28 The Court of Appeal held that the inconsistency did not arise as article 7 had no application to "inter-citizen" disputes. The officials implementing the prohibition order were not acting on behalf of the Government, but pursuant to a court order made at the instigation of a private individual against another private individual.

Storage

5.29 Information privacy is based on the recognition that an individual should have some control over the dissemination of information relating to him. The Purpose Specification Principle and the Use Limitation Principle together require that data subjects should be informed of the purpose for which personal information is collected and that it should be used in accordance with that stated purpose. To ensure that this occurs it is necessary to protect the security of collected data. This aspect is covered by the OECD Security Safeguards Principle. This states:

---

4 [1992] 1 HKLR 185.

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

5.30 This principle emphasises the responsibilities of record holders, as it is they who determine the method of storage ranging from manila folders in an unlocked box to a sophisticated automated system. There is currently no statutory or common law provision specifically requiring that reasonable safeguards be employed to protect personal information, so that confidential records may end up in rubbish dumps, or faxes may be left lying around in open office areas. The tort of negligence provides a remedy only where negligent storage results in foreseeable financial loss and therefore falls far short of the ambit of the Security Safeguards Principle.

Data subject access and correction rights

5.31 The OECD Individual Participation Principle, it will be recalled, provides that:

"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."

5.32 The OECD Expert Group considers these rights as "perhaps the most important privacy protection safeguard."[5] At the emotional level it reduces the sense of powerlessness of those whose lives are recorded, for increasingly such records have tremendous influence over them. At the

[5] OECD, *op cit*, see note 1, paragraph 58.

practical level, such rights of access and correction are vital management tools in enhancing the accuracy of records relied upon in decision making.

5.33 There is no general common law right entitling a person to see and to correct records pertaining to or affecting him, either generally or specifically. To remedy this situation, many common law jurisdictions have legislation providing rights of access in particular contexts. In the public sector context, for example, the United States, Canada, Australia and New Zealand have "freedom of information" legislation creating a right of access to information held by most public authorities regarding their activities. But as regards specified categories of information, Hong Kong is still governed by an enactment with precisely the reverse effect, namely the Official Secrets Act 1989. As regards personal information, many jurisdictions have legislation providing data subjects the right of access to and correction of records relating to them. It may be contained in general data protection legislation, or in legislation targeting a particular sector. The records of credit agencies, for example, are the basis for decisions on whether or not to extend finance. If such records are not disclosed and inaccuracies corrected, people may be erroneously and unfairly denied credit. However, Hong Kong presently has no legislation providing protection against defective credit records nor in any other sphere of private sector activity, exacerbating the lack of more general data protection legislation. To date, data subject access and correction rights have received no legal recognition in Hong Kong.

No prospect of major common law developments

5.34 Having looked at the extent to which there currently exist in Hong Kong legal provisions, either statutory or common law, giving effect to the internationally agreed data protection principles, we turn now to the need for legislative intervention. Before doing so, however, the potential contribution of the courts requires consideration. The question was addressed in *Kaye v. Robertson*,[6] discussed above at paragraph 4.5. The English Court of Appeal there held that the right to privacy had been disregarded for so long by the English common law that it could now only be recognised by the legislature. It is accordingly unrealistic to expect the courts to intervene at this stage. In any event, it is doubtful if a court would be equipped to formulate a comprehensive data protection model.

Voluntary data protection guidelines as an interim measure

5.35 It is clear from the foregoing that to date the data protection principles have not been incorporated into Hong Kong's domestic law. This is not to say, however, that these principles have not been accorded any official recognition in Hong Kong. In 1988 the government issued, with the approval of the Executive Council, a booklet entitled "Data Protection Principles and Guidelines" to major computer users in the private sector. A circular

[6] [1991] FSR 62 (CA).

memorandum to similar effect was issued to government departments and agencies. Dated 17 March 1988, it notes that the government has been monitoring overseas developments and "has accepted in principle that data protection should be introduced". As an interim measure, however, it commends computer users to voluntarily comply with certain data protection principles.

5.36 The principles described cover much the same ground as the major international formulations, particularly the OECD Guidelines. A detailed comparison of their texts is set out in the next chapter. The voluntary principles are articulated and described in the context of promoting good data protection practice. It is made clear that they have no legislative effect, but adherence is "invited" on a voluntary basis. Nor do they envisage full compliance. The Explanatory Memorandum accompanying the voluntary guidelines comments, for example, that "full compliance at present with the subject access principle is not expected." The exercise will have an educative function by promoting adherence to the principles and should facilitate the introduction of legislation. For the sake of completeness, however, the feasibility of continuing to rely on the present voluntary system is now examined.

Feasibility of continued reliance on voluntary guidelines

5.37 For the purposes of the present discussion, a voluntary regime is one that lacks mandatory statutory controls. As such, it saves costs and avoids red tape. Despite these attractive features, the Canadian, Australian and United Kingdom law reform inquiries that have examined the matter have unanimously concluded that this approach provides inadequate protection to privacy. The United Kingdom Committee on Data Protection ("the Lindop Committee") considered that "a wholly voluntary approach would not suffice ... [The] public will, we believe, look ... for an assurance that data protection can, in the last resort, be enforced."[7] That committee reported in 1978 and the international trading impetus for the adoption of domestic legal protection has increased since then.

5.38 The views of other law reform agencies are persuasive, but available empirical evidence on the effectiveness of voluntary regimes is also relevant. This is difficult to obtain for:

> *"in reality self regulation may equal no regulation and just provide a convenient tool to hold out and proclaim that something is being done about data protection. It may be quite difficult to determine in each case whether the self regulation is effective or nothing more than paying lip service to data protection."*[8]

---

7 *Report of the Committee on Data Protection* (Chairman: Sir Norman Lindop), Cmnd. 7772, 1979.

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

New South Wales: a case study

5.39 A useful "inside" view of the effectiveness of a voluntary regime is provided by the New South Wales Privacy Committee. This is a statutory committee independent of government. It has issued voluntary guidelines and acts as a privacy ombudsman in investigating complaints arising under them. This is obviously a much stronger voluntary model than Hong Kong's. The inclusion of a privacy agency (unlike Hong Kong) means that in New South Wales there is a means to monitor the effectiveness of a system lacking legally enforceable controls. It is therefore significant in our view that a recent annual report[9] concludes that:

> *"If Parliament wants to ensure that technology is used for the benefit-not the detriment-of society then ... it must be prepared to establish a mandatory framework to control the processing of personal data ..."*

5.40 A major inquiry subsequently (and quite independently) completed in New South Wales has highlighted the extent to which privacy protection is eroded in the absence of enforceable controls. In its two year inquiry, the New South Wales Independent Commission Against Corruption exposed a widespread corrupt trade in the unauthorised release of government information.[10] It found that information from a variety of State and Commonwealth sources, as well as the private sector, had been freely and regularly exchanged and sold over many years. Much of the information was of a sensitive nature and with obvious commercial value. The report noted that "commercial interest has prevailed over commercial ethics; greed has prevailed over public duty; laws and regulations designed to protect confidentiality have been ignored."[11] It reported that the corrupt trade had been allowed to flourish because:

> *"(i) There has not in the past been any consistent policy to determine what information should, and what information should not, be available to the public.*
>
> *(ii) Access to information that has been publicly available has frequently been associated with such delay that a parallel illicit trade has developed, with greater speed its prime selling point.*
>
> *(iii) Information that has been held as confidential, has generally not been well protected. Rudimentary*

---

9 New South Wales Privacy Committee Annual Report 1989.

10 New South Wales, Independent Commission Against Corruption; *Report on Unauthorised Release of Government Information*, August 1992.

11 *Ibid,* Volume 1, Chapter 1, page 3.

precautions have not been taken with the systems that have been in place."[12]

5.41 Assistant Commissioner Adrian Roden QC urged in his report that immediate and effective action be taken to deal with the problem. He states:

"Much more is needed than a punitive response to disclosed corrupt conduct. The whole question of management of the increasing amount of confidential information held by the Government and its agencies, is in need of urgent attention. Until there are clear policies, adequate protection and effective laws, cherished privacy principles will be at risk, and the scope for widespread corruption will remain."[13]

5.42 The Report identifies three areas for remedial action:

"1. There must be a clear line drawn between information which is available to the public, and information which is retained as confidential.

2. That which is available to the public, should be readily, quickly and cheaply available.

3. That which is to be retained as confidential, should be properly protected."[14]

Conclusion

5.43 This case study of the ineffectiveness of a voluntary regime further argues for the adoption of data protection legislation. We conclude that the effective protection of information privacy is essential for Hong Kong and that this requires legislative intervention. **We recommend that the internationally agreed data protection guidelines be given statutory force in both the public and private sectors.**

12 *Op cit*, Volume 1, Chapter 1, page 9.
13 *Ibid,* Volume 1, Preface.
14 *Ibid*, Volume 1, Chapter 1, page 8.

Chapter 6

The Standards to be Applied

Summary

6.1 All data protection legislation is founded on a set of data protection principles. This chapter looks at the three most influential sets of principles, namely those contained in:

(i) the Council of Europe Convention on data processing, which are the basis for various European data protection laws;

(ii) the OECD Guidelines, which are the basis for the laws in a number of countries, including Australia and Japan, and the voluntary guidelines in Hong Kong; and

(iii) the draft Directive which differs from the other two major formulations in that it not only lays down a set of principles but also requires a data user to satisfy one of a number of grounds for data processing. It also provides a comprehensive set of requirements which Member States should include in their data protection legislation.

Recommendations

6.2 We recommend the adoption of the OECD Guidelines. Insofar as that formulation differs in substance from the Hong Kong voluntary guidelines, we recommend that preference be given to the OECD formulation (Paragraph 6.4).

Comparison of texts of OECD Guidelines and Hong Kong voluntary guidelines

6.3 We set out below a comparison between the texts of the OECD Guidelines and the voluntary guidelines. The latter guidelines are those which were issued by the Hong Kong Government in 1988 to both the private and public sectors. These do not have legislative force but are intended as a guide to good data protection practice. They are broadly based on the OECD Guidelines but differ in some respects.

	OECD Guidelines	*Hong Kong Voluntary Guidelines*
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 or consent of the data subject.	There should be limits to the collection of personal data; such collection should be fair and lawful and, where appropriate, with the knowledge or consent of the data subject.
Data Quality Principle	Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up to date.	Personal data should be adequate, relevant and not excessive in relation to the purposes for which they are to be used. Personal data should be accurate and, where necessary, 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 fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.	The purposes for which personal data are collected should be specified not later than at the time of data collection; subsequent use of personal data should be limited to the fulfilment of legitimate purposes already specified or such other as are not incompatible with them.

	OECD Guidelines	*Hong Kong Voluntary Guidelines*
Use Limitation Principle	Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except: (a) with the consent of the data subject; or (b) by the authority of law.	The purposes for which personal data are collected should be specified not later than at the time of data collection; subsequent use of personal data should be limited to the fulfilment of legitimate purposes already specified or such others as are not incompatible with them. Personal data should not be disclosed for purposes other than those which have been specified 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.	Personal data should be protected by appropriate safeguards against unauthorised access, alteration, disclosure or destruction and against accidental loss or destruction.
Openness Principle	There should be a general policy of openness about developments, practices and policies relating 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.	There should be a general policy of openness about developments, practices and policies with respect to personal data.

	OECD Guidelines	*Hong Kong Voluntary Guidelines*
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 subparagraphs (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.	At reasonable intervals and without undue delay or expense, a person should be able to obtain confirmation of whether or not personal data are held of which he is the subject, to have communicated to him any such data in an intelligible form and, where appropriate, to have such data corrected or erased.
Accountability Principle	A data controller should be accountable for complying with measures which give effect to the principles stated above.	-----

6.4 **We recommend the adoption of the data protection principles as set out in the OECD formulation. Insofar as that formulation differs in substance and not merely semantically from the voluntary guidelines, we prefer the OECD formulation.** In our view its articulation of several of the principles is more stringent and precise. Nor do the guidelines possess an equivalent of its Accountability Principle, presumably because the omission of a data controller is inherent in a voluntary system. More fundamentally, we prefer the OECD formulation precisely because it represents an international consensus on the appropriate standards.

6.5 The precise wording in legislation implementing these principles will be a matter for the Law Draftsman. We note that the United Kingdom Data Protection Act contains a guide as to how the very generally worded principles (based on those of the European Convention) should be interpreted.

It has been pointed out[1] that "the inclusion of such a guide is most unusual in terms of the normal structure of United Kingdom legislation." An alternative approach is that of the Australian Privacy Act 1988. This fleshes out the principles instead of separating their statement from their interpretation.

The draft Directive

6.6 The draft Directive proposes the most detailed regulatory framework formulated to date addressing the protection of personal data. References in this report to the text of the draft Directive are to the revised draft issued on 15 October 1992. The structure of the draft Directive is complex. Unlike the OECD Guidelines, it does not restrict itself to an articulation of data protection principles. The core concerns of the OECD data protection principles are addressed by the Directive provisions, but often with reference to mechanisms and procedures aimed at giving them effect. In this respect the draft Directive resembles a data protection law and, indeed, many of its provisions derive from those found in European data protection laws. We have recommended the adoption of the OECD Guidelines rather than the later draft Directive because the Guidelines provide in our view a clearer statement of the underlying principles, without the quasi-legislative detail of the draft Directive. In addition, Hong Kong has already adopted the OECD Guidelines as the basis for the administrative guidelines on data protection which were issued by the Government in 1988. In the remainder of this report we examine how to give these principles practical effect and the relevant draft Directive provisions are examined in this context.

6.7 The draft Directive's concern with the implementation of the data protection principles is supplemented by article 7's articulation of the grounds on which personal data may be lawfully processed. This provides as follows:

> ***Principles Relating to the Grounds for Processing Data***
>
> ***ARTICLE 7***
>
> *Member States shall provide that personal data may be processed only if:*
>
> *(a) the data subject has consented;*
>
> *(b) processing is necessary for the performance of a contract with the data subject, or in order to take steps at the request of the data subject preliminary to entering into a contract;*

[1] Tim McBride, *Data Privacy: An Options Paper,* (Ministry of Justice, New Zealand, 1987), paragraph 13.21.

(c) processing is necessary in order to comply with an obligation imposed by national law or by Community law;

(d) processing is necessary in order to protect the vital interests of the data subject;

(e) processing is necessary for the performance of a task in the public interest or carried out in the exercise of public authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary in pursuit of the general interest or of the legitimate interests of the controller or of a third party to whom the data are disclosed, except where such interests are overridden by the interests of the data subject."

6.8 The OECD Guidelines contain no equivalent to article 7. They attempt to provide a self-standing set of minimum standards for the protection of information privacy. Their application is not limited by particular data processing purposes as such. The draft Directive goes further and superimposes upon the requirements of the principles the additional requirement that the processing must be necessary for stipulated purposes, unless the data subject consents. The language employed by article 7 is necessarily general, but as explained in Chapters 10 and 11, it includes the aim of regulating data purposes that envisage decisions adversely affecting the data subject. The remaining chapters address the requirements of both formulations in their examination of appropriate legal controls on the processing and use of personal data. For the purposes of discussion the different stages in the data processing cycle are distinguished. Accordingly there are separate chapters dealing with collection, use and disclosure, data subject access and correction rights, and storage security and accuracy. This approach is taken for convenience only, and we agree with the OECD that "it is essential that the principles are treated together and studied as a whole."[2] Many of the mechanisms discussed assume the existence of an enforcement agency. The functions and powers of such an agency are discussed in a later chapter, as are exemptions and transborder data flows.

[2] OECD Guidelines, *op cit*, paragraph 55.

Chapter 7

Data Protection Laws in Other Jurisdictions

Summary

7.1 This chapter looks in broad terms at the incidence and principal features of data protection laws overseas. Five features of particular importance in those laws are identified. These are whether the law;

(i) covers both automated and non-automated data;

(ii) is to be enforced by a data protection agency or the individual himself;

(iii) covers both the public and private sectors;

(iv) provides mandatory enforcement powers to a supervisory authority; and

(v) requires data users to obtain approval to process personal data from the supervisory authority.

Data protection overseas

7.2 The following 27 jurisdictions have enacted data protection laws.[1] A number of the laws came fully into force a year or so later than the date of enactment of the legislation, sometimes in stages:

Jurisdiction	year came into force
Australia	1988
Austria	1978
Belgium	1994
Canada	1982
Czechoslovakia	1992
Denmark	1978
Finland	1987
France	1978
Germany	1977
Guernsey	1986
Hungary	1989

[1] *Transnational Data and Communications Report*, March 1994, at 42.

Iceland	1981
Ireland	1988
Isle of Man	1986
Israel	1981
Japan	1988
Jersey	1987
Luxembourg	1979
Netherlands	1988
New Zealand	1991
Norway	1980
Portugal	1991
Spain	1992
Sweden	1973
Switzerland	1992
United Kingdom	1987
USA	1974

7.3 European jurisdictions predominate to date, although North America is also represented. The only Pacific rim countries with data protection legislation are Australia, New Zealand and Japan.

7.4 In addition to these countries which have enacted laws on the matter, a number of others are actively considering legislation. Bills have been prepared in Greece, Italy, and Taiwan.[2]

7.5 A data protection law is one that enforces the data protection principles as regards personal information records. How that is achieved differs from one system to another. Some of the most significant differences are examined in the following paragraphs.

Data to be regulated: automated and/or non-automated

7.6 Data protection laws focus on the regulation of data representing personal information. They vary in the extent to which they allow the data storage medium to restrict their scope. Accordingly some laws only regulate automated data, whereas others also encompass non-automated data.

Enforcement: by data subject litigation or an enforcement body

7.7 With the sole exception of the USA, the different laws establish a specialised body to concentrate on the task of overseeing the enforcement of the data protection principles. The laws variously describe the agency as a "Data Protection Commission", "Privacy Commission", or similar. (For convenience, this report will refer to the regulatory agency envisaged for Hong Kong as the "Privacy Commissioner". This does not of course pre-empt the

[2] *Transnational Data and Communications Report*, *op cit.*

adoption of a more suitable term at a later date.) To equip them to discharge their enforcement role, the regulatory agencies are conferred powers of varying width regarding such matters as inspection of data users. These bodies also assist the data subject to protect his rights, through a complaints investigation mechanism. Usually investigation procedures are exercised as informally as circumstances permit. Formal powers are generally conferred, however, to provide a legal backup when required. There is usually a right of appeal to the courts and occasionally to an independent tribunal as well.

Public and private sector regulation

7.8 European data protection laws usually apply to both the public and private sector. The USA, Canadian and Australian federal laws, however, only regulate the public sector. This is partly explained by constitutional constraints inhibiting federal jurisdictions from legislating to regulate the private sector, although the United States and Australian federal governments have enacted legislation to regulate specific private sector records, such as credit records.

Advisory or mandatory enforcement powers

7.9 A further distinction between the laws is that some countries have opted to confer mandatory powers on their enforcement agency, whereas others restrict it to an advisory role. An example of the former approach is the United Kingdom Data Protection Act. Enforcement powers are exercised by the Data Protection Registrar, including the function of registering data users. By issuing a de-registration notice he renders illegal the holding of personal data. By way of contrast, Germany's Data Protection Commission has the power to investigate and persuade, but not to issue binding instructions. If a data user fails to comply with the Commission's complaint, the Commission must seek to pressure it to do so by reporting the matter to the Parliament and hence the media. In a robust democracy such as that country possesses, such a system is as effective as the mandatory model.

Approval requirement for data users

7.10 As indicated by the example given above, a feature of some mandatory models is a requirement that data users obtain approval from a central authority. The last decade has witnessed a general movement away from such "licensing" or "registration" requirements, as these approval requirements are generally known. The 1988 Netherlands law, for example, only requires data users to notify the supervisory authority of their activities, but consent is not required. Also, the recent Home Office review of the United Kingdom Data Protection Act has rejected that legislation's emphasis on registration of data users. It is increasingly recognised that requiring the data

protection authority to approve all users diverts its resources from other activities better suited to achieve compliance.

Policy convergence

7.11 This chapter has focused on some of the differences between the various data protection laws. It is fitting, however, to conclude by noting the striking extent to which the data protection laws of diverse countries correspond. Professor Colin Bennett[3] has comprehensively analysed this issue of policy convergence from the perspective of a political scientist. He identifies a number of forces accounting for this convergence across national boundaries. The interaction of these forces with the beliefs and institutions of the different countries accounts for the divergence outlined above.

[3] *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, (Cornell, 1992).

Chapter 8

The objectives and scope of a data protection law

Summary

8.1 This chapter considers the scope of a law giving effect to the data protection principles and concludes that such a law should be concerned with "personal data", in the broad sense of any representation of information relating to an identifiable individual.

8.2 The data protection principles described in earlier chapters effectively constitute a code of fair information practices. They recognise that decisions affecting data subjects are made on the basis of data available to the data user. That data may be factual or judgemental, true or false. Data may relate to the data subject's private life, such as his sexual habits, or to his public self, such as his nationality. We conclude that a data protection law cannot therefore restrict its attention to intimate data.

8.3 The chapter also looks at the medium in which data are stored. We note that some data protection laws elsewhere are restricted to automated data. We reject this option as we believe that *any* data may influence a decision maker's treatment of the data subject and the medium in which they are stored is irrelevant. In addition, we believe that restriction of the law to automated data would give scope for evasion and fail to take account of the continued dominance of manual records in Hong Kong.

Recommendations

8.4 There should be legal regulation of all data representing information or opinion, whether true or not, which facilitates directly or indirectly the identification of the data subject to whom it relates (paragraph 8.17). The data to be regulated must, however, be disposed in such a way as to enable access to required data to be practicably obtained by automated or manual means (paragraph 8.35). However, all data (regardless of its level of retrievability) must be protected by reasonable security safeguards (paragraphs 8.36).

8.5 The data protection principles should immediately apply to data in existence upon enactment of the law, subject to there being a transition period of one year before:

(i) the data quality principle applies. There should be no right to compensation for a breach of this principle during this period.

(ii) the subject access provisions fully apply. The data user would not be obliged to provide a full copy of all data held at the time of the request, but would be entitled first to clean up the data by updating and removing irrelevant or dubious data. He would then be obliged to provide the data subject with a copy of all the remaining data. Upon expiration of the transition period he would lose the right to alter data before responding but would be required to provide a copy of all the data held upon receiving the request (paragraph 8.38).

All personal data to be legally regulated

8.6 We recommend below the legal regulation of all personal data. The expression "personal data" merits some explanation, however, and both "data" and "personal" require separate analysis:

(i) "Data" means the representation of information. "Information" is the interpretation that an observer applies to the data. As Professor Wacks explains:

> *"A good deal of the literature treats 'information' as interchangeable with 'data'. It may, however, be useful to distinguish between the two. 'Data' become 'information' only when they are communicated, received and understood. 'Data' are therefore potential 'information'. Thus when the data assume the form of the printed word, they are immediately transformed into information by the reader. Where, however, data consists in acts or signs which require any meaning, they remain in this state of pre-information until they are actually understood by another."*[1]

"Data" has a wider meaning than "information". By definition, encrypted data do not constitute "information". It will be seen below that data protection laws seek to regulate data representing personal information, rather than attempting to apply directly to such information.

(ii) "Personal" in this context means data relating to an identifiable individual. "Personal data" encompasses all such data relating to an individual. It includes but is not restricted to data of an intimate or sensitive kind.

---

1 Wacks, *op cit*, page 25.

8.7 It follows that for the purposes of regulation "personal data" refers to any data recording information relating to an identifiable individual, no matter how apparently trivial. Professor Wacks, however, defines "personal information" as follows:

> *"'Personal' information consists of those facts, communications, or opinions which relate to the individual and which it would be reasonable to expect him to regard as intimate or sensitive and therefore to want to withhold or at least to restrict their collection, use, or circulation."*[2]

8.8 We have considered whether the law should only regulate data representing "personal" information in this sense of connoting intimate information. As Professor Wacks notes, "if a loss of 'privacy' occurs whenever *any* information about an individual becomes known (the secrecy component) the concept loses its intuitive meaning."[3] This raises fundamental questions regarding the objectives of an information privacy law.

Objectives of an information privacy law

8.9 Flaherty has commented that "although the general inspiration for the development of data protection laws is apparent, the goals are rarely spelt out in satisfactory detail."[4] Nor does the literature address the question very precisely, but as data protection laws give effect to the data protection principles, their aims can be discerned from an examination of those principles.

Regulation of data representing information

8.10 The first feature that is apparent about the data protection principles is that they address themselves in terms to data rather than apply directly to the information represented. This will, however, effect the legal regulation of the personal information represented by the data. The principles recognise that the personal data thus regulated is often recorded with some degree of permanence. They refer to the collection of data, of it being provided reasonable security safeguards, of the appointment of data controllers, and the right of data subjects to have communicated in a readily intelligible form data relating to them. This focus on recorded data contrasts with the common law duty of confidence described in Chapter 4. That duty is addressed to any information disclosed in circumstances imposing the obligation, whether orally or recorded. So in *Stephens v. Avery*[5] it was held that the duty attached to the disclosure of information orally imparted in confidence. The disclosure was not of recorded data. Data protection laws

---

2 Wacks, *idem.*

3 Wacks, *ibid*, page 16.

4 David Flaherty, *Protecting Privacy in Surveillance Societies* (University of North Carolina Press, 1989), page 30.

5 [1988] 2 All ER 545.

regulate the disclosure of recorded information, although the disclosure itself may be in any form, including orally.

8.11 The data protection principles are much broader than the duty of confidence. They provide protection from a number of perils to personal data, including for example unfair collection methods and insecure storage methods, as well as improper disclosures. The duty of confidence is restricted to this latter concern. In this regard, however, its operation partially complements that of the Use Limitation Principle. We saw in Chapter 4 that insofar as the duty of confidence operates to protect from unauthorised disclosure personal information (as opposed to its more usual staple of trade secrets), this protection tends to arise in the course of legally recognised relationships, such as doctor and patient. The data protection principles regulating disclosure apply regardless of such relationships. The common law duty provides protection against unauthorised disclosure where the confider deals directly with the recipient. Data protection laws go further and seek to address modern society's propensity to store and disseminate personal data by record keepers usually lacking personal knowledge of the data subject. In such circumstances the record keeper's knowledge of the data subject will be restricted to the record and disclosure will be limited to that record. Should the record keeper orally add extraneous comments about the data subject which do not constitute part of the record, these comments will only become subject to the data protection law if the recipient records them. Upon being so recorded, the information becomes a candidate for reference and regular disclosure to third parties. Oral comments which are not given permanent form are of more fleeting impact.

Fair information practices

8.12 In addition to being largely about personal information records, data protection laws are concerned with fair practices in handling the information so recorded. The combined effect of the principles has been described as ensuring that the right information is disclosed to the right person for the right purpose. They also provide data subjects with a degree of control over data relating to them, with rights of access to and correction of such data. Data protection laws are accordingly about fair information practices, not as an end in themselves, but because it is recognised that *decisions* are made on the basis of that information affecting data subjects. There is a similarity between data protection laws and the common law rules of procedural fairness known as the rules of natural justice. These common law rules have been summed up as providing that "persons must be afforded a fair and unbiased hearing before decisions are taken which affect them."[6] The data protection principles also provide a "right to be heard", although it is more limited than that afforded by the rules of natural justice. Although they do not provide that a data subject has the right to provide an input prior to the data user making adverse decisions affecting him (such as denial of credit), access and correction rights enable him to provide periodic inputs. In Chapter

[6] M. Aronson & N. Franklin, *Review of Administrative Law* (Sydney: The Law Book Company Limited, 1987), page 91.

11 we go further and recommend that prior to the implementation of an adverse decision the data subject should be afforded the opportunity to correct the data. The data user will not, however, be required to divulge factors not contained in the data.

Informational self-determination

8.13 A third general objective that can be discerned from the data protection principles is an emphasis on the data subject having a degree of control over data relating to him. As the OECD puts it, data protection laws generally aim to ensure "to the greatest possible extent individual awareness, participation and control."[7]

Regulation of sensitive information insufficient

8.14 It follows from this analysis that data protection laws cannot restrict their attention to sensitive or intimate data, because decisions drastically affecting the data subject may be made on the basis of data lacking these qualities. Terrorists have been known to locate targets through address listings in telephone directories. It is the context which determines the potential impact of an item of information. It is also true, however, that some categories of data are particularly prone to expose persons to adverse and, more specifically, discriminatory decisions. These are recognised in article 8 of the draft Directive. This declares:

> *"Member States shall prohibit the processing of data revealing racial or ethnic origin, political opinions, religious beliefs, philosophical or ethical persuasion or trade union membership, and of data concerning health or sexual life."*

8.15 This provision goes on to list a number of conditions permitting the processing of such data. It envisages *additional* protection for those classes of information which may be the basis of discriminatory policies (as Milan Kundera has written[8], "the struggle of man against power is the struggle of memory against forgetting"). Such an approach is examined in Chapter 9, but for present purposes the important point is that the Convention is not *restricted to* such information. On the contrary, it applies the data protection principles to "any information relating to identified or identifiable individuals" and it characterises such information as "personal data". This approach is shared by all data protection legislation enacted to date.

8.16 A further reason why it would be impractical to restrict a data protection law to intimate or sensitive data is that data are cumulative. The accumulation of trivial data can result in the compilation of revealing profiles. Individual purchases may for example tell one little about a person, but a

---

7 OECD Guidelines, *op cit,* paragraph 5.

8 Kundera, *The Book of Laughter and Forgetting*, London: Penguin Books 1980.

comprehensive record over a period of time will describe the consumer's lifestyle.

8.17 For these reasons we agree with the approach invariably adopted elsewhere and recommend that **all data representing information or opinion, whether true or not, which facilitates directly or indirectly the identification of the data subject to whom it relates be regulated by law.** A "data subject" must be a living individual as it would be too complex to extend regulation to the estates of deceased persons. This formula encompasses both the situation when the data subject's identity is determinable from the data alone, and that when his identity can only be established by combining it with other information.

8.18 It should be noted that there are definitional problems regarding "sensitive" data which, although not insurmountable, do complicate the application and hence administration of a data protection law. These are addressed below when we examine the issue of whether there should be additional protection for certain categories of data.

Factual and judgmental data

8.19 Information about a person may be strictly factual and objective, such as a date of birth. Often, however, it includes an opinion or judgment. To say that a person drinks a bottle of brandy daily is an assertion of fact, but one inviting the judgment that the person is an alcoholic. The distinction is often a matter of form and difficult to draw. Also, we have noted above that data protection laws are concerned with material upon which decisions are made affecting the data subject. Judgmental data will often be more influential in this regard than the factual basis it purports to convey. Accordingly, we have recommended above that legal regulation of personal information encompass both factual and judgmental data. This is the approach generally adopted by existing data protection laws.

Incorrect data

8.20 Data may be false and judgments may be erroneous. Such incorrect data will nonetheless influence decision makers to the detriment of data subjects. It follows from the concern of data protection laws with fair information practices that they must cover all personal data, regardless of whether the data purport to be strictly factual or contain an evaluative aspect. Indeed, the Openness Principle confers on data subjects the right to challenge faulty data. The Australian Privacy Act 1988 explicitly (and we think usefully) recognises this by defining "personal information" as information or an opinion "whether true or not".

8.21 The application of the data protection principles to both inaccurate and accurate data demonstrates that the principles extend beyond the protection of privacy as such. "Privacy" is generally thought to relate to

protection from the disclosure of accurate information about a person. The distinction is recognised by the common law which limits a remedy in Hong Kong for defamation to false statements injurious to reputation. It is a complete defence that the statement is true. The data protection principles do not advert to this distinction.

Relevance of data storage mediums

8.22 Data may be recorded on paper, microfiche, computer tape, optical disc, or elsewhere. Our approach is to focus on data records regardless of the storage medium. Some data protection laws, however, have concerned themselves with distinctions between different data storage mediums. We therefore address the issue whether the regulation of personal data should be limited to a particular storage medium. For the purposes of discussion it therefore becomes necessary to advert to distinctions such as those between automated and non-automated (also known as "manual") data, despite their artificiality. There are several alternative approaches:

(i) only cover non-automated data. We are not aware of any data protection law which is restricted in this manner. In view of the computer boom such a restriction would drastically limit the law's effectiveness and we reject this option.

(ii) only cover automated data. This is a common approach, approximately half of the countries with data protection laws having restricted them in this manner. The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data specifically countenances regulation being limited to automated data. A number of European data protection laws nonetheless chose to also encompass manual records.

(iii) cover personal data, regardless of the recording medium. This is also a common approach, being adopted by the remaining half of countries with data protection laws. This broad approach is adopted in the OECD Guidelines. It has been endorsed by the draft Directive. Article 3 provides that it shall apply to the processing of personal data "wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which forms part of a file or is intended to form part of a file." A "file" is defined as a structured set of personal data accessible according to specific criteria.

The need to regulate non-automated data

8.23 To restrict a data protection law to automated data would in our view seriously limit its effectiveness. The reasons for encompassing all recorded data regardless of form are as follows:

Principle not form

8.24 In principle we reject a restriction based on the storage medium of the data. The data protection principles are concerned with any data that may be taken into account in decisions affecting the data subject. The storage medium of the data is irrelevant to this issue, subject only to the fact that storage mediums vary in their efficiency in retrieving data. Unlike automated data, manual data may be impossible to locate, due to the records being insufficiently organised. To accommodate this point, we recommend below that the law only apply to data which are reasonably readily retrievable, regardless of the medium in which they are held. This is subject to the exception we explain at paragraph 8.36 that the requirement to keep data securely applies to all data, regardless of the data's level of retrievability.

Operational interrelationship between mediums

8.25 One of the reasons cited by the OECD Expert Group for not limiting their Guidelines to the automatic processing of data was difficulty in clearly distinguishing between automatic and non-automatic handling of data. They noted that there are "mixed" data processing systems.[9] The definitional difficulties are accentuated by ongoing technological developments. There is an increasing operational interrelationship between the two mediums. When formulating proposals in an area such as this, it is vital that they are not prone to being out-stripped by developments in technology. This was a point emphasised to us in discussions in mid-1991 with international experts. Some have predicted that with the increased use of optical scanners the practical distinction between manual and computerised records will disappear by the end of the century. Professor Simitis referred to the tagging of computerised records with cross-references to relevant manual records, creating mixed systems. To the same effect, a European Communities Commission spokesperson explaining the coverage of structured manual files commented that with new techniques such as increasingly powerful data bases and scanners, unstructured manual records could more easily become structured.[10]

Manual records still dominant in public sector

8.26 In Hong Kong, non-automated records still dominate in the public sector. The total quantity of records held by government agencies totals some 900 kilometres. Furthermore, the present annual growth rate is 16%.[11] Files comprise 54% of this total and only 1% is machine readable. Although rapid computerisation of new government records is under way,

---

9 OECD Guidelines, *op cit*, paragraph 35.

10 *Privacy Laws & Business Newsletter* (October 1990), page 5.

11 Hong Kong Standard, 26 March 1994.

clearly the failure to apply the law to non-automated records would emasculate public sector regulation for the foreseeable future.

Opportunity of evading regulation

8.27 Restricting regulation to computerised information provides record-keepers with the opportunity for circumvention. This was a concern of the OECD Expert Group who noted:

> *"by exclusively concentrating on computers the Guidelines might lead to inconsistency and lacunae, and opportunities for record-keepers to circumvent rules which implement the Guidelines by using non-automatic means for purposes which may be offensive."*[12]

Circumvention may be effected by moving personal data from databanks onto manual records or simply refraining from computerising manual information. There is evidence that the latter is occurring with United Kingdom employment-vetting agencies, for example.[13]

Much information recorded manually

8.28 Often it is the more intimate information which is recorded on non-automated paper files. This is also the position in Hong Kong. Mrs Patricia Chu, a senior officer in the Social Welfare Department and a member of the sub-committee, advises that most of the often sensitive personal information held by the Social Welfare Department is contained in paper files. We consider the UK experience instructive in this regard. The Data Protection Act 1984, contrary to the recommendations of the Lindop Committee, restricted its attention to the automatic processing of data. Subsequent enactments in 1987, 1988, and 1990, however, have granted access and correction rights to manual records relating to social services, housing authorities and health records. This ad hoc approach has been criticised[14] on the grounds that this supplementary legislation fails to apply a coherent set of data protection principles or provide a regulatory agency. As the Data Protection Act does possess these features, the data subjects of computerised records enjoy greater protection than those recorded in manual files. The simpler and more effective solution is to apply the same regulatory framework to both computerised and structured manual records.

Manual records and retrievability

---

12 OECD Guidelines, *ibid*, paragraph 35.

13 R. Norton-Taylor, *In Defence of the Realm?* (London, The Civil Liberties Trust, 1990), pages 72-3.

14 *New Law Journal*, 5 October 1990, page 138.

8.29 Non-automated records range from the systematic to the shambolic. The extent to which they are kept in an organised manner is generally related to the readiness with which information on particular data subjects can be retrieved. This is relevant to the degree of risk posed of disclosure to third parties. A person referred to in passing in a lengthy criminal investigation report, for example, is less vulnerable to that information being passed on than where the information is part of indexed or cross-referenced paper records. This is relevant because disclosure is a main concern of data protection laws and, indeed, privacy. As previously mentioned, data protection laws are also concerned with records being used as the basis for decisions affecting data subjects. Information relating to a data subject buried in an amorphous file and effectively irretrievable as a result is less likely to provide a basis for decisions affecting him by the record-keeper. The same retrieval difficulties reduce the incidence of its transmission to other decision makers. This focus on data that occasions specific risks to the data subject is reflected in the OECD Guidelines. The explanatory Memorandum comments on this that:

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

8.30 Turning from principle to practicability - and the practicability of our proposals is of vital concern to us - we are concerned that to apply all the data protection principles to data which are not reasonably retrievable would be unduly onerous for record keepers. The most obvious difficulty would arise in relation to the application of the access principle, which could result in the record keeper having to sift through large amounts of material for scattered references to the data subject.

8.31 It is for reasons such as these that, although the majority of data protection laws are not restricted to automated records, many do not encompass all non-automated records. Different formulations are used, but their aim is to restrict protection to organised non-automated records. This is the approach adopted by the draft Directive which extends to non-automated processing of personal data forming part of a "personal data file." This is defined by Article 2 as:

> *"Any structured set of personal data, whether centralised or geographically dispersed, which is accessible according to specific criteria and whose object or effect is to facilitate the use or alignment of data relating to the data subject or subjects."*

8.32 We agree with this approach for a law covering both the public and private sector. If only public sector regulation was envisaged, consideration would have to be given to a more stringent standard which put the onus on record keepers organising their records. This has been the Canadian approach, for example. This may well be a major undertaking for the Hong Kong government, as we have been advised that some departments

have seven or more independent manual record systems. We are conscious also, however, that our recommendations propose a new set of obligations for the private sector as well. Many will be small record keepers who will have disorganised paper records. Our terms of reference task us to formulate proposals for the protection of privacy and not the betterment of records management for its own sake. We note, however, the concern expressed by the Legislative Council Panel on Information Policy that users could avoid the application of the law by refraining from organising their records in a systematic manner. This followed from the fact that we were not recommending that data users be required to re-organise their data to facilitate the data's ready retrievability. If not so organised, the law would only apply if and when the data were used. There was no telling when this could occur. Data mismanagement would accordingly obstruct access and correction rights. Although we do not consider it feasible to apply the law generally to non-retrievable data, it does highlight the extent to which records management will impact on the implementation of the law.

8.33 Although it is conventional to think of data as being read, we do not consider relevant the perceptual sense employed to interpret the data. It follows that data should be regulated whether they appear on paper, microfiche, computer tape, audio tape, video tape, optical disc, film, or any other data storage medium that may be devised. Given the rate of technological change we are anxious to avoid definitions tied to specific technologies which are vulnerable to being outstripped by future developments.

8.34 While in principle we consider that identical controls should apply regardless of the form of the data, we recognise that at the operational level distinctions may be required. Access requirements will, for example, have to accommodate the different mediums of storage.

8.35 We received few submissions objecting to the proposal in the Consultative Document to regulate both automated and retrievable manual data. **We have concluded that the new data protection law should apply to personal data in whatever form held so as to enable access to required data to be practicably obtained by automated or manual means.** While this recommendation broadly follows article 2(b) of the draft Directive, we have not referred to a "structured set of personal data" nor to the Consultative Document's "organised collection of data". The key issue is, it seems to us, whether or not the data in question can readily be retrieved, regardless of the extent to which the data may or may not be "structured". We also depart from the draft Directive in referring to *enabling* access, rather than *facilitating* it. Our formulation is therefore somewhat narrower, connoting as it does making access possible rather than merely easier.

8.36 **Our recommendation in the preceding paragraph is subject to the exception that the obligation to keep personal data protected by reasonable security safeguards imposed by the OECD Guidelines' Security Safeguards Principle should extend to *all* personal data, regardless of the data's level of retrievability.** We think it reasonable that

all holders of personal data should be required to take reasonable precautions to prevent "such risks as loss or unauthorised access, destruction, use, modification or disclosure of data". We discuss this in more detail in chapter 12.

Existing records/transition period

8.37 The Consultative Document proposed that the legislation provide a transition period, but did not specify its length nor provide further details. Understandably, respondents sought clarification. The most extreme position, was that the law should only apply to personal data generated after the law is enacted. We reject this option for automated data on practical grounds, as well as on grounds of principle. As to the former, it would be operationally difficult, if not impossible, to distinguish data held before and after a particular date. As a matter of principle, we are not prepared to permanently deny access and correction rights to existing data. Further, excluding existing holdings from the application of the law would severely limit its scope, sanctioning the continued retention and use of data not collected or maintained in accordance with the principles. Distinguishing between data on the basis of the storage medium and providing a transition period for manual data would also have drawbacks. It would encourage data users to retain sensitive data on manual files, thereby eluding the application of the law during that period. This would also have the undesirable consequence of generally delaying the computerisation of records.

8.38 On the other hand, we recognise that updating and purging data in both manual and automated form will be a major undertaking, but a major aid to the upgrading of data quality will be provided by data subjects exercising their access and correction rights. It would be unfair, however, to subject data users immediately to the full force of the law. They should be provided the opportunity to put their data in order before becoming liable to pay compensation. **We accordingly recommend that the data protection principles should immediately apply to data in existence upon enactment of the law, subject to there being a transition period of one year before:**

(i) the data quality principle applies. There should be no right to compensation for a breach of this principle during this period.

(ii) the subject access provisions fully apply. The data user would not be obliged to provide a full copy of all data held at the time of the request, but would be entitled first to clean up the data by updating and removing irrelevant or dubious data. He would then be obliged to provide the data subject with a copy of all the remaining data. Upon expiration of the transition period he would lose the right to alter data before responding but would be required to

provide a copy of all the data held upon receiving the request.

Exemptions

8.39 We have defined above the recommended scope of the data protection law. It should be borne in mind that this discussion is in general terms. In Chapter 15 we make detailed recommendations on the exemption from regulation of a number of data purposes. Some of these are of broad application, in particular the recommended total exemption of data held solely for personal and domestic purposes.

Chapter 9

Collection of personal data

Summary

9.1 The processing of personal data begins with its acquisition or collection. In this chapter, "collection" means the obtaining of personal data from the data subject, whereas by "acquisition" we mean obtaining data relating to the data subject from third parties. Data may be collected from the data subject with his active co-operation, such as where he provides answers to questions, or without, such as where a utilities meter provides information automatically to the utilities company. Where he initiates the collection himself, the data subject may not appreciate the extent of the data collecting capabilities of the equipment he is using.

9.2 The data collection principles require that limits be set on the collection of personal data. We address the need to restrict collection or acquisition of data to that which is relevant to the data purpose. The principles also require that collection methods should be fair. Fair consensual collection requires that the data subject be informed of relevant matters, such as the purposes for which the data is sought and its intended recipients. These requirements need adjustment when data is collected from the data subject without his knowledge or consent. We consider, but reject, a requirement of collection only from the data subject, which would exclude acquisition of personal data relating to him from third parties. While the Collection Limitation Principle does not apply to data acquired from third parties (a point not made clear in the Consultative Document), such data is subject to the Use Limitation Principle discussed in the next chapter. A later report will make more specific recommendations on when it is permissible to collect data without the individual's knowledge or consent but once collected, it is subject to the application of the other data protection principles, subject to any exemptions applying.

9.3 Personal data may be sensitive because it pertains to intimate aspects of the data subject's private life, such as his health. Alternatively, while it may relate to more public aspects of the data subject, such as trade union membership, it may expose him to discriminatory decisions. We consider but reject controls on the collection of such data.

Recommendations

9.4 We recommend that the broad principles contained in our scheme should be supplemented by more detailed sectoral codes of practice. These codes of practice should not be given legal force, nor the power to

qualify the provisions of the data protection law, but compliance with a sectoral code approved by the Privacy Commissioner should be taken into account in determining whether there has been a breach of the principles (paragraph 9.9).

9.5 We recommend adoption of the OECD Collection Limitation Principle. This provides that:

> *"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 or consent of the data subject"* (paragraph 9.11).

The law should provide that personal data shall not be held or collected or held unless:

(a) the data are collected, acquired or held for a lawful purpose directly related to a function or activity of the collector; and

(b) the collection, acquisition or storage is necessary for, or directly related to, that purpose. (paragraph 9.15).

When data are collected with the knowledge of the data subject, he should upon the first collection be informed about:

(a) the purpose of the processing for which the data are intended;

(b) the obligatory or voluntary nature of any reply to the questions to which answers are sought;

(c) the consequences for him if he fails to reply;

(d) the recipients or categories of recipients of the data;

(e) the existence of a right of access to and rectification of the data relating to him; and

(f) the name and address of the controller and of his representative if any.

Items (a) to (d) should be specified upon the collection of the data. As for (e) and (f), it should be sufficient if the data subject is informed of these by the time that the data are used (paragraphs 9.23 and 9.24). While (a), (d), (e) and (f) must be made explicit, (b) and (c) need not be made explicit when obvious (paragraph 9.25). Where the data user collects data from the same individual on more than one occasion, he should take reasonable steps to remind him of these matters from time to time (paragraph 9.26).

9.6 A data subject from whom data are collected without his knowledge through automatic metering should be informed of the frequency of

data collection, the time of their storage, and the use to be made of the data. If this is not feasible, the collection of data should be subordinated to legal authorization (paragraph 9.28).

9.7 A data subject from whom data are collected by automated means which he initiates should be provided the following safeguards:

(a) the data subject's consent should be required prior to the installation of the relevant technology in real or personal property under his control.

(b) only personal information which is necessary for service or billing purposes should be collected and stored (paragraph 9.30).

Codes of Practice

9.8 Before examining in detail the controls we propose on the collection of data, we should explain at the outset that our proposed scheme is intended to provide a broad and flexible framework based on the principles of the OECD Guidelines. We intend that that scheme should be supplemented by more detailed provisions contained in separate codes of practice drawn up to reflect the particular circumstances of particular sectors. We recognise, however that data uses differ between sectors. The data protection principles are flexible enough to accommodate this. Data purposes differ between sectors and the Purpose Specification Principle acknowledges this. We agree with the UK Registrar's views on the appropriate status of codes:

> *"Some suggest that detailed statutory codes should be prepared for each sector and that compliance with such codes should replace compliance with the data protection principles.*
>
> *I have come to disagree with that view. The great effort required to define sectors and develop precise codes in fine detail would, in my view, divert resources from encouraging compliance with the powerful and flexible Principles. The Principles give a broad basis on which the Tribunal and courts can build. They are flexible enough to take account of sectoral differences, the variation of individual cases and the development of new technologies.*
>
> *On the other hand, there is a role for codes of practice as a guide to compliance with the Principles. I recommend that the Registrar should have power to give formal endorsement to codes so that they could have a similar force to the Highway code. Thus, compliance with or breach of a code would be*

taken into account by the Tribunal but breach of a code would not of itself amount to a breach of a principle.[1]

9.9 We agree with this approach. **We recommend that sectoral codes of practice should not be given legal force, much less the power to qualify the provisions of the data protection law. However, compliance with a sectoral code approved by the Privacy Commissioner should be taken into account in determining whether there has been a breach of the principles.**

9.10 Notwithstanding the limited legal scope of sectoral codes, we wish to emphasis that we consider their development a vital feature of a comprehensive data protection scheme. In Chapter 4, for example, we gave the example of how a code is needed to flesh out the complex legal issues associated with AIDS. The data protection principles are necessarily very general. While this approach provides flexibility, codes can usefully furnish more specific guidance by elaborating on the principles.

OECD Collection Limitation Principle

9.11 **We recommend adoption of OECD Collection Limitation Principle. This provides that:**

> ***"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 or consent of the data subject."***

9.12 This principle addresses several main concerns. The first is with limiting the extent of collection. By "collection" is meant collection from the data subject. This was not made clear in the Consultative Document. The acquisition of data from third parties does not constitute "collection" in the sense that we use that term in this chapter. The second is the legitimacy of the means employed to obtain data within those limits. Related to this is the role of consent. Before these aspects are examined, it should be noted that comprehensively identifying the circumstances where the data subject's knowledge or consent is "appropriate" will be deferred to the second part of the reference.

Limiting the extent of collection

Only necessary data to be collected

9.13 The principle refers to "limits to collection", without specifying them. The Explanatory Memorandum to the OECD Guidelines, however, states that it relates to "the collection of data which, because of the manner in

[1] Fifth Report of the Data Protection Registrar, June 1989, London: HMSO, paras. 236-238.

which they are to be processed, their nature, the context in which they are to be used or other circumstances, are regarded as specially sensitive."[2] This aspect is considered below. We also consider an important limit to collection to be that of relevance. This is specified in the Data Quality Principle which states in part that "personal data should be relevant to the purposes for which they are to be used." The Explanatory Memorandum accordingly discusses this requirement in that context. It is also relevant to the present discussion, however, that data should only be collected from the data subject or acquired from third parties if the data are relevant and therefore *necessary* for their proposed purposes. So the Canadian and Australian federal legislation, for example, explicitly provides that personal information shall *not* be collected unless it is directly related to a function of the collector. That legislation relates solely to the public sector. Article 7(e) of the draft Directive is to similar effect. It provides in part that processing (defined to include collection) should be "necessary for the performance of a task in the public interest or carried out in the exercise of public authority vested in the controller or in a third party to whom the data are disclosed."

9.14 We agree that it is important to properly constrain public authorities in acquiring personal information because, as Chapter 3 demonstrates, they are often statutorily empowered to compel disclosure. In theory, an applicant for a private sector benefit such as a loan may refuse to disclose personal information of no relevance to the application. The reality will be that applicants will feel constrained to provide all the information the service-provider deems useful, actually or potentially. This pressure will be even more pronounced in monopoly or cartel situations. On the other hand, the need for organisations to be informed of all information of direct relevance before granting a benefit or service will condition an applicant's legal right (in the absence of compulsory statutory requirements) to refuse to divulge it.

9.15 In view of the above, we favour statutory recognition being given to the requirement that only relevant information be collected in both the public and private sectors. **We accordingly recommend that the law should provide that personal data shall not be collected or held unless:**

(a) the data are collected, acquired or held for a lawful purpose directly related to a function or activity of the collector; and

(b) the collection, acquisition or storage is necessary for, or directly related to, that purpose.

The role of declarations

9.16 As discussed below, we propose that all record keepers compile a declaration specifying their functions and activities. This will be a public document which will fulfil various verification functions, including compliance with the requirement recommended above that data collection or acquisition

[2] OECD Guidelines, *op cit*, paragraph 50.

be directly related to the collector's functions. One of the aspects requiring description in a declaration are the purposes for which data are kept.

Fair and legitimate means of collection

9.17 The OECD principle requires that data should be collected by "fair and lawful means." The Explanatory Memorandum gives as examples of contraventions of this limb the use of hidden tape recorders or obtaining data by deception. The two distinct concepts of lawfulness and fairness will often overlap in their application, but they are conceptually distinct. In the Hong Kong context, "lawful" would mean neither prohibited by statute nor a civil wrong. The latter includes a breach of contract or the equitable duty of confidence. The applicable principles were discussed in Chapter 4. But added to this requirement of lawfulness is the positive requirement of *fair* means of collection. Fairness depends on the circumstances and cannot be spelt out in detail.

Purpose Specification Principle

9.18 The Collection Limitation Principle adds that collection should be "where appropriate, with the knowledge or consent of the data subject". This knowledge or consent cannot operate in a vacuum however: it must relate to the purpose for which the data are collected. The Purpose Specification Principle is relevant as it provides that:

> *"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 of purpose."*

9.19 It follows that if data are to be collected from the data subject with his knowledge and consent, he must be informed of their proposed uses. The two requirements of knowledge and consent are linked, as uninformed consent is no consent.

Consensual collection: informing data subjects of relevant matters

9.20 Article 11 of the draft Directive addresses the extent to which there should be legislative provision to ensure that data subjects from whom data are collected are informed of relevant matters, namely:

> *"(a) the purpose of the processing for which the data are intended;*
>
> *(b) the obligatory or voluntary nature of any reply to the questions to which answers are sought;*

(c) the consequences for him if he fails to reply;

(d) the recipients or categories of recipients of the data;

(e) the existence of a right of access to and rectification of the data relating to him; and

(f) the name and address of the controller and of his representative if any.

2. Paragraph 1 shall not apply to the collection of data where to inform the data subject would prevent the exercise of or the co-operation with the supervision and verification functions of a public authority or the maintenance of public order".

9.21 Submissions from direct marketing organisations pointed out that the provision does not explicitly state when the data subject will be so informed. The Consultative Document suggested that the data user should not have to inform the individual at the outset, provided he does so at some later stage. We think, however, that there are practical difficulties in not requiring that data subjects be informed of *any* of matters (a) to (f) *upon* collection. Requirements (b) and (c), in particular, only make sense at the stage when the data subject is determining whether or not to volunteer the data. The other matters will also be relevant to his decision about this. This is evidently what the revised Directive has in mind, as its Explanatory Memorandum comments on the requirement that:

"if personal data are to be collected fairly and lawfully the data subject must be able to decide whether or not to disclose data relating to him in full knowledge of the purposes of the processing, the existence or otherwise of a legal obligation to disclose the data, and the consequences for him if he fails to reply. To ensure that he can defend his rights and monitor the use of data relating to him he should also be informed of his rights of access and rectification, and given details of the recipients of the data."

9.22 This comment suggests that the matters adverted to in the first sentence be communicated to the prospective data subject at the outset, whereas the other matters can be communicated later. This would appear logical because the data collector may not have initially identified the recipients, and rectification rights are standard.

9.23 **We therefore recommend that the following matters should be specified upon the collection of the data, as being directly relevant to the individual's decision whether or not to respond:**

(a) the purpose of the processing for which the personal data are intended;

(b) the obligatory or voluntary nature of replying;

(c) the consequences for him of failing to reply; and

(d) the recipients or categories of recipients of the personal data.

9.24 **That leaves (e), requiring that the data subject be told of access and correction rights, and (f), requiring contact details of the data controller. We recommend that it be sufficient if the data subject is informed of these by the time that the data are used.** We recognise, however, that from the data user's point of view it will often be more convenient to advise the data subject of *all* these matters (i.e. not only (a), (b), (c) and (d) but also (e) and (f)) at the outset. We also fear that a two-step process could annoy customers.

"Obvious" matters

9.25 Direct marketing respondents submitted to us that there should not be a requirement to make explicit matters that the context makes obvious, or that the individual may know from other sources. Our concern, however, is that a data purpose which is "obvious" to one person may not be to another. We recognise, however, that the obligatory/voluntary nature of replying and the consequences of failing to reply will often be obvious. For example, it will be obvious that to respond to an advertisement is voluntary. Equally obvious will be the consequences of failing to respond (i.e. not receiving the product or service). **We accordingly recommend that items (b) and (c) at para. 9.20 above need not be specified when obvious, but that the data subject must be explicitly advised of items (a), (d), (e) and (f).**

9.26 The remaining aspect requiring consideration is whether the individual must be informed of all these matters upon every collection. It was pointed out to us that with frequent collections such as occur with medical treatment this would be impracticable. **We accordingly recommend that the data user must advise the individual of all these matters upon the first collection and upon further collections should take reasonable steps to remind him of them from time to time.** Should the data purposes change, the data subject must of course be immediately told.

Non-consensual collection: new technologies

9.27 Article 11 addresses the matters that a data subject must be informed of when the data collection requires his co-operation. Its reference to questions and replies conveys that it is primarily concerned with the conventional consensual collection methods requiring an active rather than a

passive data subject. But new technologies increasingly facilitate the collection of data in novel ways. The metering of the use of public utilities may occur without the data subject's direct involvement. The problem is not adverted to in the draft Directive (other than providing an exemption in article 11(2)), but has been addressed by the Council of Europe.[3] It recommends that individuals subjected to "remote" monitoring should be informed of the frequency of data collection, the time of their storage, and the use to be made of the data. If this is not feasible, the collection of data should be subordinated to legal authorization. The recommendation goes on to prohibit the secondary use of the data and to require erasure within a limited time. These latter requirements are implicit in the other data protection principles and will be dealt with below. The recommendation also refers to access, but this is also covered by article 13.

9.28 We propose that the collection of data from data subjects by automatic means should be regulated. As with our other recommendations, however, we are concerned to avoid formulations which are technology-bound. **We therefore recommend a provision along the lines of that recommended by the Council of Europe to deal with automatically metered collections from the data subject without his knowledge. This will ensure that although his consent is not required to the collection process, he will be informed. It is accordingly a weaker requirement than the one we have recommended for consensual collections from the data subject.** To impose the stricter requirement could unduly inhibit the operation of public utilities. Also, to the extent that the data subject will usually be in a contractual relationship with the data collector, his consent to the collection may be implied. We note that the OECD principle only requires the data subject's knowledge or consent "where appropriate." The Explanatory Memorandum elaborates that knowledge is a minimum requirement but consent cannot always be imposed for practical or policy reasons, such as in criminal investigation activities.

9.29 The Consultative Document similarly proposed but adopted the Council of Europe's terminology of "remote" collections. This vague expression elicited concern from some respondents, as suggesting a wider application than was the case, and prompted our more precise reformulation.

9.30 Another data collection method increasingly displacing the conventional question and answer approach involves automated collections initiated by the data subject. For example, by engaging in a telebanking transaction the customer releases data which will be stored for services and billing purposes. Although unlike metered collections the data subject initiates the collection process, this does not ensure that he is aware of the data collecting capabilities of the equipment concerned. For example, television receivers now come equipped with microchips which automatically collect data on such items as the identity of video cassettes played. The stored data may then be accessed from a remote point. As these functions are activated by the mere use of the equipment, the operator will be oblivious of them

[3] Council of Europe, *New Technologies: A Challenge to Privacy Protection*, Strasbourg: 1989.

unless (and we think this unlikely) he was informed of them upon purchase. The commercialisation and misuse of the data thus collected pose data protection dangers. A sectoral form of regulation has been adopted in Germany to address the problems. That would provide the most comprehensive response. In the meantime, however, **we endorse the recommendations of the Council of Europe on the collection problems posed by this new approach (known as "interactive media"). In particular:**

(a) the data subject's consent should be required prior to the installation of the relevant technology in real or personal property under his control; and

(b) only personal information which is necessary for service or billing purposes should be collected and stored.

9.31 Regarding (a), we have specifically not restricted this requirement to the installation of technology in the data subject's residence. The installation of new technologies is not confined to a person's residence but may, for instance, apply to his vehicle. The recent introduction in Hong Kong of automated collection of tunnel tolls is but one example of data collection outwith a person's residence by automated means.

New technologies, surveillance, and our Reference

9.32 The applications of these new technologies for the collection of personal data may constitute a form of surveillance. It differs only in degree from traditional methods such as bugging. We are reporting specifically on surveillance and intrusion in a later document. Insofar as surveillance results in the retention of data, that data will be the subject of the other data protection principles, subject only to any applicable exemptions.

Matching of data previously collected from the data subject

9.33 The Council of Europe has expressed concern about organisations matching data on various files relating to the one data subject on the ground (among others) that:

> *"Accumulating data in this way excludes the data subject from the information circuit. It is no longer necessary for a particular administrative body to contact the individual with a view to acquiring information or checking information he has already furnished."*[4]

[4] Council of Europe, *The Introduction and use of Personal Identification Numbers: The Data Protection Issues*, 1990, Strasbourg.

Data-matching: a paradigm of using pre-collected data

9.34 The general question of data matching is considered in Chapter 11. For present purposes, the relevant point is that matching of pre-collected data obtained in different contexts may weaken the requirement that collection be with the data subject's knowledge and consent. Compared with fresh collection, it is also prone to problems regarding the meaning and quality of the data being matched. Jon Bing's example of the Kungsbacka municipality in Sweden is instructive:

> *"Files were matched in order to identify persons receiving housing aid (a special social benefit) to which they were not entitled. Approximately 1,000 persons were identified and reported to the police. Of these, 1/4 could be discarded out of hand as above suspicion. A rather large fraction of the rest were convicted in the first instance court, but acquitted at the next level. A total of 10-20 individuals were actually convicted of social security fraud.*
>
> *"The explanation was simply that different definitions of 'income' had been used in the files matched - it is, of course, well known that there are differences between 'gross income', 'net income' and so on. Swedish law actually contained more than 25 different definitions of income. Matching them resulted in inappropriate inferences."*[5]

9.35 Jon Bing has identified the factors favouring the use of previously collected information.[6] Such pre-collected information is readily accessible. Fresh collection from the data subject will require the additional time needed to complete the application form or record the interview. Further effort may be required to interpret the information with respect to the applicable criteria, whereas pre-collected data will typically be pre-classified. We note, however, that as appears from the Kungsbacka example, the use of (and in particular the matching of) pre-recorded data may adversely affect data quality. The pre-collected data may have been classified according to different criteria, so that incorrect inferences may be drawn from such data. Data collectors will have to bear this in mind if they wish to avoid the sanctions described below for the storage and disclosure of inaccurate data. Our detailed recommendations on data matching also address some of the problems.

A legal requirement of collection from the data subject?

9.36 In view of the above, we have considered the related question of whether there should be a legal requirement that data about an individual must be collected only from him, not acquired from third parties. We note that

---

5 Jon Bing, Working Paper prepared for the Conference on Information Law Towards the 21st Century, Amsterdam, June 1991.

6 Bing, *ibid.*

the draft Directive and existing data protection laws do not so provide. The German Federal and State Data Protection Commissioners have expressed the view, however, that the Directive "should be clear that personal data have to be collected directly from the data subject."[7] The acquisition of data by third party transfers is widespread, however, and it may be neither realistic nor indeed practical to attempt to ban them. Although not subject to the Collection Limitation Principle, such transfers are subject to the use Limitation Principle discussed in the next chapter.

Restricted collection of special categories of data

9.37 Information which is not collected cannot of course be subsequently processed or disclosed. We now address the issue of whether there are any special categories of data which merit controls on their collection and therefore their subsequent use.

9.38 We concluded in Chapter 8 that a data protection law should regulate all data relating to an identifiable individual. This recommendation on the scope of regulation recognises that even apparently trivial data may be used to the detriment of the data subject, depending on their context. We noted, however, that some data protection laws accord *additional* protection to special categories of data. These categories of data are accorded special treatment on the basis of their "sensitivity." Whilst even apparently innocuous data may assume sensitivity in a particular context (such as an estranged spouse's address), the sensitivity of these special categories of data is less dependent on context. To take one generally accepted category of sensitive information as an example, information relating to one's sexual life is considered inherently "personal" in the sense of intimate. Further, it retains this quality in all contexts, as Professor Wacks's following example shows:

> *"Naturally X may be more inclined to divulge, say, his extra-marital affair or his homosexuality (or both) to his psychiatrist or to a close friend than to his employer or his wife. And his objection to the disclosure of the information by a newspaper might be expected to be even stronger. But the information remains 'personal' in all three contexts. What changes is the extent to which he is prepared to permit the information to become known or used."*[8]

OECD Guidelines

9.39 We referred earlier to the OECD principle's reference to "limits to collection" and the Explanatory Memorandum elaborates that collection should be limited to data "which because of the manner they are to be processed, their nature, the context in which they are to be used or other circumstances are regarded as especially sensitive." It explains that the

---

7 *Transnational Data and Communications Report* (March 1991), page 45.

8 Wacks, *op cit*, page 23.

Expert Group had not found it possible to define any set of data which are universally regarded as sensitive. It has therefore contented itself with the general statement that there should be limits to collection "to represent an affirmative recommendation to lawmakers to decide on limits which would put an end to the indiscriminate collection of data".[9] One of the relevant considerations in such an exercise was the "traditions and attitudes in each member country."

Draft Directive

9.40 Article 8 of the draft Directive goes further than the OECD principle and expressly restricts the processing (including collection) of the following special categories of data:

> *"data revealing racial or ethnic origin, political opinions, religious beliefs, philosophical or ethical persuasion or trade union membership, and of data concerning health or sexual life."*

Establishing the sensitive categories of data

9.41 Article 8 of the draft Directive restricts the processing of two conceptually distinct categories of "sensitive" information. These are intimate data and data likely to be utilised in discriminatory decisions.

9.42 **Intimate data** Professor Wacks has developed a threefold classification of the sensitivity of data as high, moderate or low. Of particular relevance in the present context is his definition of "high sensitivity" data:

> *"These are in general, intimate data about an individual, relating in particular to some facts of his medical history, sexual behaviour, or other aspects of his life which may accurately be described as 'private' or 'personal'. It is in respect of this class of information that the 'privacy' argument is strongest, and there is a persuasive case for maintaining that at least some of these data should not be collected at all."*[10]

9.43 It is commonly pointed out that notions of the sensitivity of data are culture-bound. For example, details of personal taxation and financial affairs are treated as highly confidential in the United Kingdom but are publicly available in Sweden. "Sensitivity" is not an intrinsic quality of information, but relates to the expectations of individuals. These are variable even within a specific community. Empirical data on what the Hong Kong populace considers sensitive is provided by the recent survey results which are summarised in Appendix 2.

---

9 OECD Guidelines, *op cit*.

10 Wacks, *op cit*, page 229.

9.44 A further question is whether the collection of intimate data should be limited. We have seen that the data protection principles are about fair information practices rather than the protection of privacy as such. As Professor Wacks points out:

> *"Though the ostensible objective of (data protection legislation) is normally to protect the individual's 'privacy', the very information which might be thought to warrant 'protection' in the name of 'privacy' receives little special or explicit attention."*[11]

9.45 **Data relating to discrimination** Professor Rodata usefully describes this category and its relationship to intimate data as follows:

> *"... the basis of privacy is now undoubtedly still formed by data which reflect the traditional need for secrecy (those concerning health or sexual habits for example): other categories of data have, however, come to assume increasing importance within the notion of privacy, data which are protected principally to avoid discrimination against those to whom they refer. This is mainly a matter of data regarding political or trade-union opinions, as well as data relating to race or religious beliefs. The peculiarity of this situation is born of the fact that political and trade-union opinions cannot be restricted solely to the private sphere: they are destined, at least in democratic countries, to characterise the 'public' sphere, they are among the opinions that the individual must be able to express in public, and they help to determine his 'public' identity.*[12]

9.46 The two special categories of data discussed above are not mutually exclusive. Data identifying an individual as HIV positive would be regarded as particularly intimate, as it relates to an individual's health and sexual life. It may additionally, however, prompt discriminatory behaviour by, for example, employers. To sack a person on this basis may well be discriminatory in that the condition is unlikely to affect work performance for a number of years.

9.47 This example highlights a characteristic of discriminatory decisions, namely the insufficient relevance of the information determining them. Data which are irrelevant to medium-term work performance should not usually be regarded as a decisive reason for immediately firing someone. Trial lawyers express a similar point when they describe the prejudicial value of evidence as outweighing its probative value. We have recommended above that data users be restricted to the collection of data directly relevant to their functions.

---

11 Wacks, *op cit*, page 205.

12 Stefano Rodata, *Protecting Informational Privacy: Trends and Problems,* Working Paper prepared for the Conference on Information Law Towards the 21st Century, Amsterdam, June 1991.

9.48 The issue is not as simple as this, because the relevance of any information, however sensitive, is determined by its use. To return to the HIV example, information regarding this would be highly relevant to the decision whether to provide an applicant with life insurance. Rejection by an insurer armed with this knowledge could scarcely be described as discriminatory. To deny an insurer this information would be to deny it vitally relevant material. This issue is relevant when considering whether the collection of sensitive data should be restricted.

9.49 We have discussed above the concern of a data protection law with data which is the basis of decisions adverse to the data subject. This danger is pronounced with the categories of data referred to by Professor Rodata, notwithstanding (or indeed perhaps because of) their "public sphere" nature. In our view they are comprehensively set out in article 8, namely "data revealing racial or ethnic origin, political opinions, religious beliefs, philosophical or ethical persuasion or trade union membership."

Mechanisms to restrict the collection of the special categories of data

9.50 There are several possible methods of limiting the collection of data:

(i) an outright ban on its collection;

(ii) requiring the prior approval of the data protection authority; or

(iii) requiring the prior approval of the data subject.

9.51 We reject (i) as a realistic option. Nor do we support involving the data protection authority in a consent role as this would encourage bureaucracy. The Consultative Document accordingly proposed that the prior consent of the data subject be required for the collection of sensitive data, including collection from third parties. This followed the approach adopted by article 8 of requiring the data subject's written consent to the processing (including collection) of such data.

Submissions

9.52 A number of respondents submitted that it was not practicable to require the data subject's express consent as a pre-requisite to the collection of sensitive data. The problem would be most acute when the collection was from third parties, necessitating the data subject's being specifically contacted. It was pointed out that ascertaining ethnic origin was necessary to enable mailings to be sent in the appropriate language and to facilitate targeted promotions relating to the individual's home country. More fundamentally, it was pointed out that merely asking a person's name can be equivalent to asking their racial/ethnic origin. Data on nationality are an integral requirement for banks operating in an international environment, ranging from

compliance with UN mandated sanctions to the provision of ethnically orientated products and services. Medical data on life expectancy may be relevant to lending decisions.

9.53 The submissions cited emphasize that sensitive data may be highly relevant to the legitimate functions of data users and that in such circumstances obtaining the consent of the individual should not be a pre-requisite. The ubiquitousness of ethnic data (through names) increases the difficulties of hard and fast controls at the collection stage.

9.54 Other submissions focused on the difficulties of identifying what categories of data are considered sensitive locally. The Hong Kong Christian Service pointed out that while the categories identified by the draft Directive are extensive they may not be exhaustive in the Hong Kong context. They supported additional controls, but suggested empirical research to better ascertain local sensitivities. The Society of Hong Kong Publishers "applauds the attempt to provide protection to the individual, [but] clearly it is necessary to strike a balance with the legitimate interests of commerce. If telephone number was considered sensitive, would this mean that no telephone directories would be published in future?" While this is no doubt intended rhetorically, they survey findings indicate that this is a real issue and that local sensitivities do not coincide with article 8's categories.

9.55 In view of these considerations, we have come to doubt the feasibility of a specific restriction on the collection of specific categories of data, as earlier proposed. In our view the essential issue is whether collection of the data is *relevant to* the data user's functions. We are reluctant to confer on the data subject a veto right regarding relevant data. We remain alert to the special dangers posed by the categories of data identified by the draft Directive, but prefer other approaches. In considering these, we have noted the concern of the Legislative Council's Information Policy Panel voiced at the briefing on 3 January 1994 that it is precisely the sensitive categories of data which are most likely to ground discriminatory decisions. Panel members accepted that the application of the data protection principles will set strict limits on the collection of sensitive data. Their collection will have to be relevant to the legitimate functions of the data user. Panel members' concern remained that the data subject should be equipped to verify such compliance, rather than accept it on trust. The Panel expressed support for the retention of the consent requirement, as this mechanism would ensure that the data subject could keep track of such data, facilitating targeted access requests. We have endeavoured to address this point through the use of declarations and affording the individual an input prior to the implementation of adverse decisions. We consider that these two mechanisms more efficiently address the twin concerns of monitoring the use and abuse of sensitive data than our earlier proposal of data subject consent.

Declarations

9.56 We have recommended elsewhere that all public sector data users compile public declarations specifically identifying the categories of sensitive data held. Individuals will be able to readily ascertain the contents of the declarations. Article 8's definition of sensitive data has been utilised for this purpose. Our proposals do not countenance secrecy as to the existence of data bases, although the exemptions may apply to the release of specific data. The unwarranted collection of sensitive data would be viewed by the Privacy Commissioner as a serious matter, as would the failure to disclose the holding of such data in the declaration.

Adverse decisions

9.57 We recognize that sensitive data are especially prone to be used in making discriminatory decisions. However, we prefer safeguards that focus on the impact of a decision, rather than on whether any particular category of data was utilized in reaching it.

Data processing likely to severely affect the data subject's interests

9.58 While the special categories of data discussed above are protected principally to avoid discrimination against the data subject, their processing may be innocuous. This is recognised by article 8(2) of the draft Directive. This permits the processing of sensitive data where "the processing is performed in circumstances where there is manifestly no infringement of privacy or fundamental freedoms." The accompanying Explanatory Memorandum gives as examples "the assembly of data of a political nature concerning a public representative, or the compilation of lists of persons to be approached for opinion poll purposes for a short period of time, under strict security measures." [13] Conversely, article 18(4) of the draft Directive recognises that the processing of data outside the special categories of data may nonetheless "pose specific risks to the rights and freedoms of individuals." The Explanatory Memorandum gives as examples "processing which has as its object the exclusion of data subjects from a right, a benefit or a contract." This would encompass the identification of "hits" by means of the investigative data matching techniques discussed above. Article 18 requires the prior approval of the supervisory authority to such processing. In Chapter 11 we make recommendations endorsing that requirement where the purposes of data processing, including of sensitive data, are likely to severely affect the interests of data subjects.

---

[13] Commission of The European Communities, *Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data,* Brussels, 15 October 1992.

Chapter 10

Regulation of the use and disclosure of personal data

Summary

10.1 Data is collected to facilitate its use by the record keeper, which will usually include disclosure to third parties. The data protection principles dealing with use and disclosure of personal data contain two related requirements:

(i) data purposes must be specified in writing and communicated to a third party, usually the data protection authority. This is in addition to any requirement that data should only be collected from the data subject with his consent or knowledge.

(ii) Data should only be used and disclosed in ways consistent with the specified purposes, unless the data subject's consent is obtained to the altered purposes.

Recommendations

10.2 The purposes for which 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 (paragraph 10.11).

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

(a) with the consent of the data subject; or

(b) by the authority of law, including one of the use limitation exemptions discussed in Chapter 15 (paragraph 10.35).

10.4 Users of personal data should specify all data purposes in a declaration to be furnished to the data protection authority. This would be purely a notification procedure and the Privacy Commissioner would not be required to approve the data uses (paragraph 10.21).

10.5 The Business registration scheme should be made the principal means of identifying private sector holders of personal data and bringing them within the scope of regulation. The current business registration forms should

be modified for this purpose (paragraph 10.25). The form should also alert applicants holding personal data to the need to complete a supplementary form available at the Business Registration office. This form should require the specification of data purposes and contact details of the responsible officer (paragraph 10.26).

10.6 Government and public authorities, together with private sector organisations using personal data not subject to business registration requirements, should be required to notify the Privacy Commissioner direct, by furnishing him with their declarations (paragraph 10.31).

10.7 The declaration requirement does not determine the application of the principles and users of personal data should be subject to the legal application of the data protection principles irrespective of whether they are required to furnish a declaration or whether they have done so (paragraph 10.31).

10.8 Data subjects should not be deemed to have knowledge of specified data uses contained in public declarations (paragraph 10.32).

10.9 "Data subject's consent" to a variation of data purposes means any express indication of his wishes signifying his agreement to personal data relating to him being processed, on condition he has available information about the purposes of the processing, the data or categories of data concerned, the recipients of the data and the name and address of the controller and of his representative if any. The data subject's consent must be freely given and specific, and may be withdrawn by the data subject at any time, but without retrospective effect. The consent given must relate to the specific transaction for which the data were requested (paragraph 10.39).

10.10 Each functionally distinct government department or branch and each company should constitute a separate data user (paragraph 10.41).

Specification of data purposes

10.11 The OECD Purpose Specification Principle provides as follows:

> *"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 of purpose."*

The accompanying Explanatory Memorandum elaborates that:

> *"Before, and in any case not later than at the time of data collection it should be possible to identify the purposes for which*

these data are to be used, and that later changes of purposes should likewise be specified. Such specification of purposes can be made in a number of alternative or complementary ways, e.g. by public declarations, information to data subjects, legislation, administrative decrees, and licences provided by supervisory bodies." (paragraph 54)

We recommend that this principle be given legal force.

10.12 It may be noted that all the examples given of possible ways of fulfilling the specification requirement are in writing and communicated to a third party. The Home Office came to a similar conclusion in its examination of the legal requirements of the equivalent provision in the Council of Europe Convention on Data Processing. As the Review puts it, the specification procedure "should be reasonably permanent and formal and involve communication to someone distinct from the data user himself."[1] These requirements are necessitated by the purpose of the principle:

"The need for specification of purposes cannot be met simply by telling data subjects retrospectively when they ask for information... It exists both because of the general need for openness in data use and to meet particular verification requirements: ie whether purposes are legitimate; uses and disclosures are not incompatible with the purposes for obtaining data; data are adequate, relevant and not excessive in relation to the purposes; and security is appropriate."[2]

Alternative approaches to specification of data purposes

10.13 The Home Office review also usefully identifies the various possible methods of fulfilling a requirement of notification to a third party of the specified purposes. They can be broadly categorised into two, namely notification to a central agency, and notification to other parties.

Notification to a central agency

10.14 Data protection laws commonly require data users to notify a central authority; usually an agency specially constituted to regulate data protection matters. There are several variants:

10.15 **Notification but no approval requirement** The least onerous notification requirement is one simply requiring that data users provide the agency with a copy of a declaration briefly describing its records system and in particular the purposes of its records. The agency files the document but is

---

1 Home Office, *Review of the Data Protection Act: Report on Structure,* HMSO, 1990.

2 Home Office (1990), *ibid* see note 1.

not required to approve it. The Netherlands law is an example of this approach.

10.16 **Notification coupled with approval requirement** This approach encompasses both the so-called "registration systems" and "licensing systems". The difference is that the former do not require approval prior to the processing of data, whereas the latter do. Sweden is one of the few countries with a licensing system. Registration systems are more common, and the present United Kingdom Data Protection Act adopts this approach. That statute's second data protection principle provides that "personal data shall be held only for one or more specified and lawful purposes." The UK Act's principal mechanism for the specification of data purposes is the requirement that data users notify the supervisory authority. This is effected through the interpretation clauses for these two principles providing that a "specified purpose" means a purpose described in the declaration that data users are required to furnish the supervisory authority. In view of our recommendations in the previous chapter, the data subject will be advised of this whenever the data are collected directly from him. We also recognised, however, that data may be collected from third parties. Often it will involve the transfer of pre-collected data. The record keeper may well indicate the purposes for which he is acquiring the data, but we have not recommended any general legal requirement that he do so at the collection stage. Adoption of the Purpose Specification Principle fills this gap.

10.17 **The draft Directive's mix of (i) and (ii)** Article 18 provides that data protection legislation should require that the central authority be notified of the details of data processing, including data purposes. The accompanying Explanatory Memorandum comments that the purpose must be specified before the data are collected, except where the data are collected directly from the data subject, in which case article 11 requires determination of the purpose at the time of collection (see Chapter 9). The main mechanism proposed for such specification of purposes is a requirement that the data processor furnish the supervisory authority with a written declaration describing data purposes among other things. Mere notification is insufficient and prior approval is required, for "processing which poses specific risks to the rights and freedoms" of the data subject. This provision addresses processing techniques such as investigative data matching and is examined in the next Chapter.

Notification to parties other than a central agency

10.18 The Home Office Review questions the requirement adopted by the UK Act that the data protection authority be notified of all data uses. The Home Office identifies the following alternative notification points:

(i) a statutory declaration made to a solicitor;

(ii) verification and dating of a document by a professional person such as a banker or accountant;

(iii) publication, for example in the organisation's annual report or a newspaper with a verifiable date of issue;

(iv) permanent and visible dated notices to be displayed in the organisation's shops and offices (This is slightly different from the other examples in that it provides potential rather than verified communication to a third party.); or

(v) issue of copies to data subjects. This could be upon the initial collection or at the subsequent processing stage. We discuss below the draft Directive proposal that this be an additional (instead of alternative) requirement to notification of a central authority.

Advantages vs disadvantages of notifying a central agency

10.19 The principal advantages of such a scheme which have been identified by the United Kingdom Data Protection Registrar[3] are:

(i) It can provide a list of those with whom contact should be maintained. Given the prevalence of data processing, however, government and business directories would serve almost as well.

(ii) It can produce a register which assists in directing individuals to where information pertaining to them is held. But registers have proven of little utility in this regard in the UK and elsewhere.

(iii) If accompanied by the requirement to pay a fee, the system can provide revenue.

(iv) An additional argument mentioned by David Flaherty, a critic of notification systems, is that they give the regulating agency an overview of existing information systems.[4]

10.20 The major disadvantages of requiring data users to notify a central agency is the public resources this will engage. This has proved a problem where the agency is required to approve the declarations. We do not foresee similar difficulties where this is not a function of the authority and the requirement is partially integrated into an existing administrative framework (namely business registration) as recommended below. We have, however, carefully considered the Home Office review's recommendation that not only should the United Kingdom law totally abandon its present approval ("registration") requirement, but that it should not be replaced by the requirement that the data protection authority be notified of data uses. We have also noted that the draft Directive proposal to the same effect (ie that the data protection authority be notified of data uses) has received criticism from

---

3 Fifth Report of the Data Protection Registrar, June 1985, London: HMSO, 1985.

4 David Flaherty, *Protecting Privacy in Surveillance Societies* (University of North Carolina Press, 1989).

diverse quarters, despite its lack of an approval requirement. Critics include the Ministry of the Interior of the Federal Republic of Germany[5], the European Employers Federation[6] and the International Chamber of Commerce.[7] We also note that the revised draft Directive has subsequently qualified the requirement with exceptions.

Central notification system preferred

10.21 Whilst we note these criticisms of the requirement that the data protection authority be notified of data uses, we are not persuaded by them. Accepting, as does the Home Office, that for practical as well as theoretical reasons it is essential that data purposes be specified in writing and communicated to a third party, we have no doubt that this third party should be the Privacy Commissioner. We do not consider the Home Office alternative that the data user has a wide choice in selecting the third party as viable in Hong Kong. **We accordingly recommend that users of personal data specify all data purposes in a declaration to be furnished to the Privacy Commissioner. The procedure would be purely one of notification and the Privacy Commissioner would not be required to approve the data uses.**

10.22 In determining the appropriate notification arrangements, we have borne in mind the desirability of the following features:

(i) effectiveness;

(ii) simple and appropriate procedures;

(iii) minimal cost and bureaucracy; and

(iv) the use of existing administrative systems where feasible.

Utilisation of business registration scheme

10.23 Under the provisions of the Business Registration Ordinance (Cap 310) every person carrying on any business must register his business with the Business Registration Office of the Inland Revenue Department. "Business" is defined as "any form of trade, commerce, craftsmanship, profession, calling or other activity carried on for the purpose of gain and also means a club." The procedure for registering a business is to complete the appropriate application form, depending on whether the business is carried on by an individual, body corporate, or partnership. With certain exceptions every business carried on in Hong Kong must be registered and pay an

---

5 *Transnational Data and Communications Report,* May 1991, page 41.
6 *Transnational Data and Communications Report,* March 1991, page 47.
7 *Transnational Data and Communications Report,* January 1992.

annual registration fee of $2,000 *and* a (Protection of Wages on Insolvency Fund) levy of $250.

10.24 In his submission, the Commissioner of Inland Revenue describes the procedure followed in relation to business registration ("BR") as follows. Upon receipt of the appropriate BR application form a demand note is issued by the BR Office. On payment being made by the business this demand note (bearing a cash register imprint) becomes the BR certificate and is valid for 12 months from the date of commencement of business. A renewal demand note is issued every 12 months but not a fresh application form. The BR demand note becomes the BR certificate on payment of the fee and is required to be displayed at the address of the business.

10.25 **We recommend that the Business registration scheme should be made the principal means of identifying private sector holders of personal data and bringing them within the scope of regulation.** There are over 600,000 registered businesses in Hong Kong and they would constitute the majority of private sector users of personal data. This does not include individuals using personal data solely for personal or domestic purposes, for we recommend in Chapter 15 a total exemption for this. **We recommend that all current business registration forms be modified by the inclusion of a section along the following lines:**

> ***"To comply with the Data Protection Ordinance, the following information is required from an applicant:***
>
> ***1. Name and contact details of the responsible officer under the Ordinance.***
>
> ***2. Is data relating to identifiable living individuals held by the business? [YES] or [NO]***
>
> ***3. If YES, has the purpose for which the data are held changed in the last year?"***

10.26 Hong Kong has a large number of sole proprietors, a number of whom do not hold any data relating to other identifiable individuals. We expect the majority of businesses, however, to hold personal data, such as customer lists, employee details and so on. **We further recommend, therefore, that the form should also alert applicants holding personal data of the need to complete a supplementary form available at the Business Registration office. This would require the specification of the basic features of the personal data held. The details required are set out in Chapter 13. In the present context, the relevant items are the purpose(s) for which the data are held and contact details of the responsible officer.** To ensure that requirements are kept as simple as possible, we envisage a structured multi-choice questionnaire format for mainstream data users. Data use declarations would have to be submitted to the Privacy Commissioner within 30 days of business registration. The Privacy Commissioner would send the data user a reminder if he had not

received the declaration within the prescribed period. The Privacy Commissioner would compile his own data base from all declarations received. Chapter 13 further examines the proposal for its contribution to a policy of openness about data processing. To this end, interested individuals would be provided on-line access to the contents of declarations.

10.27 We expect the above system to be simple and inexpensive. As recommended in Chapter 16, it also facilitates the imposition of a small levy which should ensure that data protection regulation in Hong Kong is self-financing. We are confident that it will avoid the bureaucratic problems that have characterised schemes requiring the approval of the authority to notified data purposes. We also expect such a system to have a number of positive benefits not referred to by the Home Office. The principal benefit for the data subject is that the centralised holding of declarations should make it easier for him to ascertain their contents and verify whether the specified data purposes are being adhered to. This verification will also assist the Privacy Commissioner in effectively discharging his various functions, including the investigation of complaints. It will also enable him to monitor the uses to which all data is put. We expect this to result in more effective regulation.

10.28 The only respondent to query the utilisation of the BR scheme in this way was the authority responsible for its administration, the Commissioner of Inland Revenue. He questioned the adaptation of the BR scheme to notify the Privacy Commissioner of personal data holdings and raised the following objections:

(i) As the BR certificate is in the form of the BR demand note with an imprint and is required to be displayed at the business address "it would seem both inappropriate and impractical for this note/certificate to be modified to include the relevant declaration." The "inappropriateness" referred to presumably arises from the Consultative Document's proposal that private sector data users be required to complete declarations describing six different matters, namely data purposes, contact details of responsible officer, data content, data subjects, data recipients, and countries data are exported to. However, for reasons explained in Chapter 13, we now recommend that private sector data declarations need only identify data purposes and contact details of the responsible officer. These simplified details will more readily be incorporated in the BR certificate. Similarly, a declaration restricted to data purposes and contact details of the responsible officer will be less susceptible to alteration than one addressing all six matters, susceptible to change from year to year, thus addressing the Commissioner's concern that the certificate is not updated annually as an annual renewal is issued instead.

(ii) The sub-committee's proposals would result in an increased workload for the BR Office to field data protection inquiries and copy the declarations to the Privacy Commissioner.

(iii) Incorporating the data protection levy in the BR fee could be resisted by businesses not holding personal data. As mentioned above, we expect most businesses to hold employee data customer lists and so on but we have received no submissions registering this objection. The Commissioner of Inland Revenue adds, however, that the increased BR fee could lead to registration defaults.

10.29 The Commissioner concludes by suggesting that the Privacy Commissioner be responsible for issuing declaration forms, collecting the levy and so forth. To facilitate this, consideration could be given to the BR Office providing details of all registrants, although the Commissioner has reservations about a resultant weakening of the statutory secrecy provision.

10.30 The Commissioner's administrative concerns raise the general issue of the distribution of work between different departments, but they have not led us to revise our opinion that the scheme we propose should be simple and inexpensive. We accordingly adhere to our earlier recommendation, subject to the simplification of the declaration form described in Chapter 13.

10.31 The scheme outlined above does not attempt to encompass all users of personal data. First, business registration does not include public sector users of personal data. **We recommend that government and public authorities be required to notify the Privacy Commissioner direct, by furnishing him with their declarations.** Second, there will be private sector organisations using personal data that for one reason or another will not be required to register as a business. We expect this group to be quite small. We recommend that they also be required to furnish the Privacy Commissioner with a declaration. There are likely to be even fewer individuals using personal data who are not required to register as a business. We recommend in Chapter 15 that individuals be exempted from the application of the data protection principles when using personal data solely for private and personal purposes. Where, however, they use data outside the scope of the exemption, we nonetheless think that such individuals should not be required to furnish a declaration. We see no reason why the data protection principles should not apply to these data users, however. It is generally recognised that a defect of the UK Data Protection law is that it ties the application of the data protection principles to the notification requirement. **We therefore recommend that all users of personal data be subject to the legal application of the data protection principles irrespective of whether they are required to furnish a declaration or whether they have done so.** As the Hong Kong Institution of Engineers points out, it would be regrettable if utilisation of the Business Registration Scheme were to obscure the point that the law is intended to apply to all data users. The scheme is merely a useful administrative mechanism.

Declarations and fair obtaining

10.32 It may assist to clarify the status of the specification of purposes contained in a declaration. In the last chapter we recommended that individuals from whom personal data are collected be informed of the proposed uses, etc. This recommendation would be unaffected by one requiring the furnishing of declarations. Even if declarations are to be public documents, it does not follow that data subjects would be deemed to have notice of their contents. The UK Data Protection Act requires such declarations to be registered, but data subjects are not deemed to have knowledge of the registered entries. **We similarly recommend that data subjects not be deemed to have knowledge of specified data uses contained in public declarations.**

10.33 A further question relating to the status of the declaration's specification of purposes would arise in the case of disputes. A data subject may claim that he was advised of proposed purposes, uses or disclosures at variance with those specified in the declaration. However, this would simply be a question of fact and not conclusively determined by the contents of the declaration.

Non-specification of "obvious uses"

10.34 In view of the requirement recommended in Chapter 9 that the purposes of data must be directly related to the functions and activities of the data user, the question arises whether there should be a requirement that even "obvious" uses be specified. The problem with such an exception is its lack of certainty and we reject it. Data users should therefore always specify their data purposes, but doing so by reference to another document would be permissible. One of the functions we envisage sectoral codes performing is defining the purposes for which personal data could be held for activites which are commonly engaged in. Those carrying out such activities could simply specify their data purposes as those applicable to the relevant activity. An example would be "data purposes of insurance companies as specified in sectoral code." It would follow that they would be restricted to such purposes failing their compiling a declaration to the contrary.

Use and disclosures to be consistent with specified purpose

Purpose Specification Principle

10.35 **The Purpose Specification Principle must be considered in conjunction with the Use Limitation Principle. We recommend adoption of this principle which provides:**

> ***"Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except:***
>
> ***(a) with the consent of the data subject; or***

(b) by the authority of law."

As to (a), we propose at paragraph 10.38 below adopting the definition of "consent" in article 2 of the draft Directive. As to (b), chapter 15 sets out the circumstances in which the data protection law should authorise disclosure contrary to the Use Limitation Principle.

10.36 The UK Act's third data protection principle is to similar effect and provides:

> *"Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes."*

10.37 This requirement that personal data should be used only in accordance with its specified purpose(s) is a lynch-pin of the data protection principles. It is important to note that the principle applies equally to the internal use of data and to its disclosure to another data user.

Data subject consent to incompatible purposes

10.38 The OECD Guidelines provide that incompatible data purposes require "the authority of law" or data subject consent. The former requirement would be fulfilled by statutory permission, including the exemptions to the principle discussed in Chapter 15. As to the latter, the Guidelines fail to spell out the meaning of consent. This omission may be remedied by reference to article 2 of the draft Directive. This defines "data subject's consent" as follows:

> *"any express indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed, on condition he has available information about the purposes of the processing, the data or categories of data concerned, the recipient of the personal data, and the name and address of the controller and of his representative if any."*

10.39 These are the matters of which data subjects should have been informed at the consensual data collection stage in accordance with our earlier recommendation adopting article 11. **We recommend adoption of this definition in article 2. We also recommend adoption of article 2's additional requirement that "The data subject's consent must be freely given and specific, and may be withdrawn by the data subject at any time, but without retrospective effect."** The consent given must relate to the specific transation for which the data was requested. An applicant for a mortgage, for instance, who consents to the use of data in relation to that transaction should not be required to consent to the data being used for direct marketing by the lender's insurance arm.

10.40 We should emphasise that we think it important that those whose consent is being sought should be on notice as to the precise nature and consequences of the consent. We would not wish to see our recommendations circumvented by the use of fine print agreements which fail to obtain genuine and informed consent from the data subject.

Disclosure distinguished from uses generally

10.41 "Disclosure" involves the transfer of data between two or more distinct data users. A number of submissions pointed out that the Consultative Document did not define "data user". One respondent suggested that the Hong Kong Government should be considered as a single data user. We disagree with this approach as it would cut across the functional differentiation of disparate government departments. In the public sector therefore, **we recommend that each functionally distinct government department or branch constitute a separate data user.** As regards the private sector, the simplest approach is to determine the matter in accordance with the legal personality of the corporation. This is in keeping with section 3 of the Interpretation and General Clauses Ordinance (Cap 1) which defines "person" to include "any body of persons, corporate or unincorporate". **We therefore recommend that in the private sector each company constitutes a separate data user.**

10.42 The OECD Guidelines subject the internal use of data by the data user and disclosure to another to the same test, namely compatibility with specified purposes. Roger Clarke points out that the Guidelines do not even mention the need for care in making disclosures.[8] The draft Directive's wide definition of "processing" similarly assimilates use and disclosure. Unlike the Guidelines and the UK Act, however, article 12 of the draft Directive, obliges the data user to satisfy himself that the data subject is informed at the time of the first disclosure of data relating to him. We note that similar notification requirements are contained in several data protection laws. The Federal Republic of Germany and the Netherlands require that data subjects be notified when data are first disclosed or stored (ie the reciprocal of disclosure). The provisions are subject to various rather generally worded exceptions, however. This may explain why people we spoke to in those two countries had only rarely received such notifications. We have considered whether to adopt also a general legal requirement that data subjects be notified when data relating to them is stored or communicated for the first time. We doubt the practicality of such a requirement and reject it.

10.43 While we disagree with article 12's approach, we have nonetheless considered whether it is appropriate for a data protection law to otherwise highlight the special responsibility arising from disclosure. We recognise that disclosure has "privacy" implications which transcend those arising from the record keeper's internal use of the data. Clarke argues that procedures need to be specified to ensure such matters as minimisation of

---

[8] Roger Clarke, *OECD Guidelines: A Template for Evaluating Information Privacy Law and Proposals for Information Privacy Law* (1988 Xamax Consultancy P/L).

the amount of data that is disclosed, rendering personal data anonymous whenever possible, and the logging of particularly sensitive disclosures.

10.44 We also note that the Australian Privacy Act 1988 recognises the additional need for care with disclosures. Thus, that Act's formulation of the Use Limitation Principle stipulates that a record keeper shall only use personal information for the purpose for which it was obtained (unless the data subject consents, to avoid an emergency, etc). We have endorsed this principle as the appropriate general limitation on the use of data. The Australian Act's definition of "use" in relation to the information "does not include mere disclosure of the information". Disclosure is dealt with in the principle as follows:

> *"Limits on disclosure of personal information*
>
> *1. A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:*
>
> *(a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency ..."*

10.45 A number of exceptions then follow. The reference to Principle 2 relates to the principle that when data are collected directly from the data subject he should be informed of the proposed purposes.

10.46 Whilst we consider that this formulation usefully highlights the special character of disclosure, we do not recommend that a provision along similar lines be adopted here. Our main concerns regarding disclosure are consistency with the data purpose and that a mechanism should exist to ensure that those to whom data are transferred are notified of corrections of inaccurate data. We recommend such a mechanism in the next chapter.

Deeming data purpose unlawful

10.47 In the foregoing discussion we have endorsed a normative approach which limits the use and disclosure of data in accordance with its specified purposes. But it does not follow that requiring data subjects to adhere to this principle will provide sufficient protection. The reason is highlighted by Roger Clarke and Graham Greenleaf as follows:

> *"The effectiveness of data protection principles is heavily dependent on the purposes for which the personal data are maintained. If data protection is to be effective, these purposes need to be decided taking into account not just the interests of the data-keeper, but also those of the individual, and society as*

a whole. This means that, in addition to internal, 'efficiency' criteria, external or 'political' criteria are needed.

Yet neither the OECD nor the Australian Law Reform Commission Guidelines provide for oversight of the purposes of personal data systems, nor disallowance of purposes. Indeed as Rule observes, such a provision is uncommon ... As a result of this lack of oversight, organisations can define for themselves their 'functions or activities', and the purposes of their data, subject only to the very remote constraint of not acting outside the law or ultra vires ... The failure of the US Privacy Act can be traced back to the token nature of control over uses."[9]

10.48 We have recommended in Chapter 9 a provision limiting the collection of data to that necessary for purposes directly related to the functions of the collector. But as Greenleaf and Clarke point out, there is nothing to prevent so broad a definition of functions (and hence purpose) that virtually any data are directly related. They give the example of the creation of one central bureau "for the purpose of gaining a complete picture of a person's socio-economic history and status, eg by pooling financial, tenancy, employment, education, medical, insurance and criminal data". The authors conclude that the OECD guidelines are defective in providing no constraints on such examples of data surveillance.

The draft Directive's more restrictive approach

10.49 It is against this backdrop that the draft Directive provisions must be considered. The Directive does not set out separately equivalents of the Use Limitation and Purpose Specification Principles. Article 6(b) provides for their combined operation, and states that personal data must be "collected for specified, explicit and legitimate purposes and used in a way compatible with those purposes." But as explained in Chapter 8, unlike the OECD Guidelines, the draft Directive's formulation of the data protection principles are not self-standing. Article 7 superimposes upon the requirements of the principles the further requirement that the processing must be necessary for stipulated purposes, unless the data subject consents. "Processing" is defined to include disclosure to other parties. Failing such consent, the processing must be necessary for:

(a) performance of a contract with the data subject;

(b) compliance with a legal requirement;

(c) the protection of the vital interests of the data subject;

(d) performance of a task of in the public interest; or

---

[9] Roger Clarke & Graham Greenleaf, *Australian Proposals to Implement the OECD Data Protection Guidelines* (1989).

(e) the pursuit "of the general interest or of the legitimate interests of the controller or of a third party to whom the data are disclosed, except where such interests are overridden by the interests of the data subject."

Data subject control over data relating to him

10.50 The conditions stipulated in (a)-(d) of the previous paragraph are narrowly stated. It is important therefore to ascertain the scope of (e), which we have quoted in full (the full text of (a)-(d) are set out in Chapter 6). The wording of (e) is very general. Nor is it to be expected that a treaty provision will have the precision appropriate to a statute. The balancing test further complicates matters. It is clear, however, that it does not confer on the data subject the right to veto the processing of data relating to him. We agree with this approach. The *Home Office Review of the Data Protection Act* addresses this issue. Although the following passage refers to the Council of Europe Convention, it is of general relevance to the issue of where to draw the line between the rights of data subjects and users.

> *"The [Council of Europe] Convention does not require that data protection legislation should give the individual an across the board control over others' use of data about him. Rather it provides that personal data may be freely held provided that (i) the purpose is legitimate-interpreted in the UK as not contrary to other legislation - and (ii) the data protection principles are complied with (eg concerning how data are obtained and handled and for how long they are held). The absence of an absolute veto or general right for the individual data subject to attach his own conditions is not accidental. The Explanatory Report to the Convention draws attention to the principle of freedom of information and makes clear that the aim is to limit it only to the extent strictly justified for the protection of other individual rights and freedoms such as the right to respect for individual privacy. Indeed, most personal data are ordinary facts about others whose circulation it would probably never have been thought appropriate in our society to restrict had it not been for the advent of computers. Furthermore, many data users depend on personal data to discharge their commercial or administrative functions effectively."*[10]

Restricting data purposes adversely affecting data subjects

10.51 While the draft Directive does not confer on data subjects a veto right on the processing of data, article 7 does impose the "bottom line" that the processing must not take place if the interests of the data processor "are overridden" by the interests of the data subject (unless it falls within one of the

[10] Home Office (1990), *op cit*, see note 1.

other five limbs of that provision). The draft Directive has other, more specific, provisions to the same effect. Article 18(4) requires the data protection authority's approval to the processing of data (whether or not sensitive) "which poses specific risks to the rights and freedoms of individuals." That provision is examined in the next chapter and we recommend its adoption. That chapter also endorses a provision requiring data subject input before adverse decisions are taken. We therefore agree with Clarke and Greenleaf on the need for oversight of those data purposes which by their very nature are likely to adversely affect the interests of data subjects. While our recommendations do not go so far as to disallow data purposes, they recognise the need for procedural safeguards such as the input of the data subject or the approval of the data protection authority.

Chapter 11

PIN's and data matching

Summary

11.1 This chapter discusses two related concerns:

(i) the information privacy implications of personal identity numbers ("PIN's"); and

(ii) the matching across databases of data relating to an individual.

11.2 The most widely used PIN in Hong Kong is the identity card number and our discussion concentrates on this. We are concerned here with the data protection dangers arising from the use of ID card numbers. PIN's constitute personal data and the use made of that data should comply with the data protection principles. PIN data should not be collected, for example, unless it is relevant to the activities of the data user. We believe that the statutory application of the data protection principles to PIN's should correct the present excessive collection and use.

11.3 The main privacy peril arising from PIN's is their role in facilitating data matching. PIN's are keys to matching across databases. Such matching may expose data subjects to adverse decisions, even where it complies with the data protection principles. This is of concern because matching is a complex process which is susceptible to error.

Recommendations

11.4 The use of PIN's should be regulated in the same manner as the use of any other item of personal data and our other recommendations should be interpreted as applying to PIN's (paragraph 11.15).

11.5 The Privacy Commissioner should promulgate a code of practice on the use of PIN's. The code should make explicit the application of the data protection principles to the use of PIN's, including the ID card number. The Privacy Commissioner should take into account the terms of the code when investigating complaints (paragraph 11.19).

11.6 Prior to the implementation of a proposed adverse administrative or private decision, the data subject must be provided the opportunity to correct, add to or erase data that form the basis of that decision, except where the proposed decision is made pursuant to, or in the course of entering into or attempting to enter into, a contract (paragraph 11.26).

11.7 Investigative data matching involving the comparison of data to identify discrepancies with a view to taking adverse follow-up action should be regulated by controls supplementing the application of the data protection principles as follows:

(i) Prior approval of the Privacy Commissioner should be required to all investigative data matching programmes, unless all the data subjects included in the programme have expressly consented. Such approval may relate only to an individual data user, or it may extend to a sector. The Privacy Commissioner should promulgate guidelines setting out the relevant factors in determining whether approval shall be granted. These will include the nature and sensitivity of the personal data, their expected accuracy, and the seriousness of the consequences of being identified as a "hit". Also relevant is whether it is proposed to inform data subjects in advance.

(ii) The guidelines should also set out procedures according "hits" the right to correct matching results before these form the basis for the taking of adverse decisions.

(iii) The onus should be on organisations to show a competing social need which overrides the privacy interests of data subjects. The justification for the data matching programme should include an outline of why alternative means of satisfying the objectives are less satisfactory, and a cost/benefit analysis of the program (paragraph 11.52).

11.8 Upon the first communication for the purpose of marketing, and at reasonable intervals thereafter, the data subject must be expressly offered the opportunity to have all data relating to him held for marketing purposes erased without cost (paragraph 11.58).

PIN's

The nature of PIN's

11.9 As PIN's relate to identifiable individuals, they constitute "personal data" in the broad sense envisaged by the data protection principles. This is so even if they are made up solely of arbitrarily assigned digits. The digits of the Hong Kong identity card number ("ID no") are not coded. Most of those European countries possessing PIN's have coded digits. However, they are composed in a manner that facilitates the individual appreciating their significance. For example, the 13 digit French PIN comprises digits denoting the individual's gender, year and month of birth, district of birth and the

sequential number on the birth register. This transparency accords with a Council of Europe recommendation on the matter.[1]

Functions of PIN's

11.10 The main purpose of a PIN is to accurately identify individuals for administrative purposes, whether it is for the issue of a travel document, a driver's licence, or a social benefit. Different PINs may be allocated for each of these purposes. Alternatively, a PIN may be multi-purpose. The Hong Kong ID card number is an example of the latter. In either case, PIN's may be more accurate identifiers than names. The Council of Europe[2] has noted that both France and Luxembourg reported that surnames and forenames are inadequate for the purposes of unambiguously identifying individuals, particularly when at stake are financial consequences (eg entitlement to allowances) or social repercussions (eg contact with police). Given the widespread duplication of Chinese names in Hong Kong, their inadequacy as identifiers is even more pronounced here. This is so whether the name is denoted by Chinese characters or in English translation.

Opposition to PIN's

11.11 A chief danger of PIN's is their potential for evolving from a specific role into a universal multi-purpose identifier. In many countries this is considered objectionable on symbolic grounds. In the Federal Republic of Germany the Constitutional Court has stated that the introduction of universal PIN's would constitute a possible attack on human dignity. One European country where such opposition is not apparent is Sweden, perhaps the only country with as pervasive a multi-purpose PIN as Hong Kong. Flaherty comments on the "remarkable tolerance" of the Swedish population for its widespread use in that country's highly developed Welfare State.[3]

PIN's in Hong Kong

11.12 In Hong Kong, as in Sweden, the ID number has become entrenched as a universal multi-purpose identifier. Hong Kong does not share Sweden's highly regulated social welfare system. Instead, the original impetus for the introduction of a universal PIN derived from Hong Kong's long standing concern about illegal immigration. Official use of the PIN has, however, rapidly spread to the private sector. This is no doubt largely attributable to the absence to date of any legislative provisions restricting the use of the ID card number. The legislation imposes a broad statutory duty to disclose it which is unaccompanied by any prohibition on its use outside the

---

1 Council of Europe, *The Introduction and use of Personal Identification Numbers: The Data Protection Issues*, 1990, Strasbourg.

2 COE (1989), see note 1.

3 David Flaherty, *Protecting Privacy in Surveillance Societies* (University of North Carolina Press, 1989).

scope of the duty. Section 3 of the Registration of Persons Ordinance (Cap 177) requires every person in Hong Kong to be registered, unless exempted. Registration entails the issuing of an identity card assigning to the individual a PIN. Section 5 requires that persons " shall in all dealings with Government ... furnish the number of his identity card to the satisfaction of the public officer requiring such number. " Through a gradual process of extension, Hong Kong residents are now routinely subjected to private sector requests for the number when completing transactions.

Dangers of PIN's

11.13 It would appear that Hong Kong people are habituated to the use of the ID card number as a multi-purpose PIN. Their tolerance may well be attributable not only to its efficiency as an identifier, but also to a lack of appreciation of the data protection dangers posed by its use. The principal danger so posed is its instrumental role in the process known alternatively as "data matching", "computer matching", or "record linkages." All three expressions refer to the process, considered in detail below, of the collation or comparison of data relating to a particular individual which is collected from different sources. When conducted by government departments the usual aim is to identify discrepancies and follow them up with administrative action. For example, a department considering an application for a means-tested benefit may check what the applicant has declared his income to be in that context against what he has declared in his tax returns. In this chapter we refer to such matching as "investigative data matching", to distinguish it from more innocuous forms. Private sector companies engaging in data matching are also concerned with building up profiles of potential customers. The matching process requires a procedure whereby the individual referred to in one set of records is inferred to be the same individual referred to in another set. The simplest and most reliable method when available is the use of a PIN, particularly when it constitutes a universal multi-purpose identifier. PINs are keys to data matching and the Hong Kong ID number is as potent as any in this capacity. As such, PIN's facilitate matching. The problem, elaborated below, is that from a data protection viewpoint data matching can adversely affect individuals in the absence of special controls.

Overseas responses to PIN's

11.14 Canada and Australia have either policy or legal controls respectively aimed at preventing the development of universal identifiers. In Canada, the Federal government issued a policy in June 1989 requiring departments to notify individuals of the purpose for which their social security number was being sought. Individuals were also to be informed whether any rights, benefits, or privileges could be withheld or any penalties imposed should they decline to disclose it. Australia has gone further and included provisions in its Privacy Act restricting the use of tax file number information. Unauthorised use of the number is a criminal offence punishable by

imprisonment. Article 8(5) of the draft Directive recognises that the use of PIN's raises significant data protection issues and provides that:

> *"Member States shall determine the conditions under which a national identification number or other identifier of general application may be used."*

The data protection principles and PIN's

11.15 A PIN such as the Hong Kong ID card number constitutes personal data, as it relates to an identifiable individual. It is therefore susceptible to the application of the data protection principles. **For the avoidance of doubt, we recommend that the use of PIN's be regulated in the same manner as any other item of personal data and that our other recommendations should be interpreted as applying to PIN's.** If our recommendations regarding the implementation of the data protection principles are given legal effect, the use of the ID number will become limited for the first time. This would effect significant (and we believe salutary) restrictions on current practices in Hong Kong. We saw above that the Registration of Persons Ordinance only imposes a statutory duty to disclose one's ID number to a public officer, yet private sector requests for this information are common. Some may furnish the number under a misapprehension that they are legally obliged to do so. Others may disclose it in the fear that their failure to do so may result in the transaction being terminated. Even when it is provided, it will usually be solely for the purpose of verification of identity. These collection problems will be mitigated by the application of our recommendations in Chapter 9 requiring that:

(i) personal data shall not be collected unless it is directly related to a lawful function of the collector. This would extend to verifying the data subject's identity should this be relevant. It would be relevant, for example, if a customer represents himself to be an account holder. It would not usually be relevant for a cash purchase;

(ii) when data are collected directly from individuals they must be informed of such matters as the purposes for which the data will be used and, unless obvious from the context, the obligatory or voluntary nature of the requests for data and the consequences if they fail to reply;

11.16 Turning to the subsequent use of the ID number for unauthorised matching purposes, this may contravene the Use Limitation Principle discussed in the previous chapter. It will be recalled that this requires that personal data shall be held only for specified purposes and shall not be used or disclosed for incompatible purposes without the consent of the data subject.

Adequacy of the principles in regulating PIN's

11.17 There are several possible approaches to the regulation of the ID card number. The most rigorous approach would be to legally prohibit its use except for limited purposes. The least rigorous approach would be to leave its control to the application of the general data protection principles. An intermediate position would be to promulgate a code of practice on the matter to supplement the general principles. This could be reinforced by the legal regulation of data matching, the principal danger posed by their use. We now set out our reasons for adopting the intermediate approach.

Legal regulation extending beyond application of the data protection principles

11.18 The legal regulation of the use of ID numbers could be in the form of a prohibition on requiring their disclosure outside the public sector. Such a provision would attempt to roll-back the present extensive use of the number outside that expressly provided for in the Ordinance. We recognise, however, that the private sector has come to rely on ID numbers where it is necessary to establish a customer's identity. We consider it neither realistic nor even desirable to curtail this use of the PIN. Adverse consequences of its disclosure, such as use for data matching, are a different matter, but this can be specifically addressed by legally regulating data matching. This is our preferred approach and our proposed controls on data matching are set out below. We consider that the disclosure of ID numbers need not be subject to specific legal regulation additional to that ensuing from the application of the data protection principles.

Code of practice regulating use of PIN's

11.19 While in principle the general application of the data protection principles should provide the necessary protection against misuse of PIN's, in practical terms more specific guidance may be desirable. The reality is that the widespread and even indiscriminate use of the ID number has become a pervasive feature of Hong Kong life. We consider that the public would be assisted by a code spelling out how the data protection principles apply in practice to the use of PIN's. This would both usefully highlight the issue, and clarify possible ambiguities. An example of the latter may be whether a legitimate purpose of disclosing an ID number should be to facilitate matching. In our view the code should explicitly exclude this. The code would not be legally binding as such. However, compliance with the code would ensure adherence to the law, whereas non-compliance would carry the risk of contravening it. **We therefore recommend that the Privacy Commissioner should promulgate a code of practice on the use of PIN's. The code would make explicit the application of the data protection principles regarding PIN's, including the ID card number. The Privacy Commissioner would take into account the term of the code when investigating complaints.**

Submissions

11.20 These recommendations reiterate the Consultative Document's proposals. A number of respondents expressed concern that they would unduly restrict their use of PIN's. We do not agree, for the essential test is simply whether the data collected is relevant. If it is relevant to verify an individual's identity and to record this process then the collection of the PIN is legitimate.

Profiling and data matching

11.21 The process of comparing or collating two or more sets of data relating to individuals collected on different occasions has two distinct forms:

(i) The collation of characteristics of various individuals to identify specific individuals. An example of this is provided by the 1973 French research project known as "Gamin." A profile of children thought to be at social and medical risk was established on the basis of a medical survey. 170 factors were identified and the resultant profile used to identify other children. A further example would be a market survey to establish the profile of the typical consumer of a particular product. It may not be restricted to data collected directly from the individual and may include third party assessments or details of transactions.

(ii) The collation of two or more sets of data relating to the same individual collected on different occasions to establish his characteristics. This is known as "data matching", "computer matching", or "record linkage". An example would be compiling a detailed consumer profile of an individual to assist in predicting his future preferences. A further example would be the taxation authority investigating tax evasion comparing what a data subject said about his income in one context with what he said in another. Indeed, "Data matching" is often used in this latter, more restricted, sense connoting the comparison of data to establish discrepancies. To avoid confusion, we will refer to this process as "investigative (data) matching."

Profiling and the draft Directive

11.22 As indicated by the above examples, "profiling" is wider than "data matching", in that it involves the combination of data from different sources relating to classes of individuals as well as to specific individuals. Like all the other forms of data processing, it is subject to the application of the data protection principles. It will be recalled that the Purpose Specification Principle requires that data purposes be specified at the time of collection.

Further, the Use Limitation Principle requires that the data shall not be used for other purposes without the consent of the data subject. The application of these principles to profiling involving data matching is examined below. In any event, Article 16 of the draft Directive takes the view that additional safeguards are warranted for profiling, whether or not it involves matching. The provision is additional to, and assumes compliance with, the data protection principles. It affords additional protection to the data subject, however, where adverse decisions are taken *solely* on the basis of the profiling results. The provision applies to all profiling, whether or not it involves data matching in the sense defined above. It provides:

> *"Member States shall grant the right to every person not to be subjected to an administrative or private decision adversely affecting him which is based solely on automatic processing defining a personality profile [unless that decision] is taken in the course of the entering into a contract, provided any request by the data subject has been satisfied, or that there are suitable measures to safeguard his legitimate interests, which must include arrangements allowing him to defend his point of view [or is authorised by a law which provides safeguards]."*

11.23 The term "personality profile" we interpret as referring to a personal profile (ie a profile relating to any aspect of an individual). This is consistent with the Explanatory Memorandum's example of the use of scoring techniques in assessing the risk of making a loan. It is important to note that this supplementary provision is limited in its application to profiling which exposes the data subject to adverse consequences. The Explanatory Memorandum gives as an example the rejection of a job application on the sole basis of a computerised psychological evaluation. It gives as an example of a decision not adversely affecting data subjects for the purposes of this provision the sending of advertising material to a list of persons selected by computer.

Submissions

11.24 The Consultative Document proposed the adoption of this requirement. The proposal was commented on by several submissions. Citibank stated that it is not uncommon for credit approval for a loan to be based on an automatically processed profile. The concern was that costs would be increased by allowing all rejected customers to put forward their point of view prior to an adverse decision being taken. This concern appears to be largely based on the belief that the bank would be obliged to disclose to customers its lending criteria. Elsewhere we clarify the point that "personal data" does not extend to criteria and hence is not subject to access rights.

11.25 The scope of Article 16 was also queried, but from the data subject's viewpoint, by the Hong Kong Council of Social Services. They questioned the relevance of the restriction of its application to a situation where the decision was made *solely* on the basis of automated processing.

The Council argued that the prevalence of manual records would lead to many decisions being taken on the basis of a combination of automated and non-automated means. We recognise that the particular concern of Article 16 is the "black box" syndrome. But we have concluded that the real issue is to afford the individual the right to correct the data before an adverse decision is implemented, whether or not it is based on a profiling process, be it automated or not. Also, retention of these limitations would provide ample scope for evading compliance.

Revised recommendation

11.26 In view of these considerations **we recommend that prior to the implementation of a proposed adverse administrative or private decision based on personal data, the data subject must be provided the opportunity to correct, add to or erase data that form the basis of that decision, except where the proposed decision is made pursuant to, or in the course of entering into or attempting to enter into, a contract.**

11.27 The deletion of the earlier proposal's reference to automated profiling has resulted in a significantly broadened recommendation. In several respects, however, additional restrictions have been imposed. Our revised recommendation replaces the reference to "a right not to be subjected to" with one providing "an opportunity" to have an input. Also, the reference to "taken in the course of entering into a contract" has been extended to an attempt to so enter, or pursuant to an existing contract. The result would be that the provision would have no application to data users with whom the individual had or was contemplating a contractual relationship. This is on the basis that if a contract is in force, it will provide a degree of protection. On the other hand, if a data user declines to enter a contractual relationship, we do not think this should activate this requirement. Of course, it would remain open to the data subject to avail himself of his general access and correction rights at any stage.

11.28 The issue is whether a broad provision to this effect is necessary. We have concluded that it is. Even if data users strictly complied with tightly drawn data purposes, data subject input may be important at the point when he is about to be affected. The decision maker's data may be outdated. Even if accurate so far as it goes, it may be incomplete and not advert to all relevant matters.

11.29 In addition to this data quality aspect is the fundamental principle that the individual should have a degree of control over data relating to him. The OECD Collection Limitation Principle provides that data should be collected with the data subject's knowledge or consent where appropriate. The revised Directive is more specific and supplements the bare principles such as purpose limitation with a number of supplementary mechanisms aimed at restricting collection and assisting the data subject in keeping track of data being circulated. We have not incorporated these controls. In Chapter 9 we abandoned our earlier endorsement of the Directive's

requirement that the data subject's express consent be required to the collection of sensitive data from third parties. Nor have we followed the Directive in requiring the data user to satisfy himself that the data subject is informed at the time of the first disclosure of data relating to him. As a result, we have not proposed *any* measures which would ensure that the data subject was aware of the compilation of third party data (e.g. neighbours, colleagues) about him and its subsequent dissemination. Our particular concern is with data which the data subject had not provided either directly to the data user, or through another data user who has passed on that information. Our proposals' failure to address this could also encourage data users to exclude the data subject from the data collection cycle, rather than be subjected to the strict requirements applying to collection directly from the data subject.

11.30 A provision providing an opportunity for input prior to the taking of adverse decisions would at least alert the data subject to data created without his participation when it came to the crunch and the data user was preparing to use the data to his detriment. As we do not think it operationally feasible to limit the provision to data collected without the data subject's knowledge or consent, the provision should extend to all data held relating to the data subject.

11.31 The recommended opportunity to provide an input has some similarity with the common law "rules of natural justice" providing a right to be heard, but it is more limited. The decision-maker is not required to divulge relevant factors which were not reduced to data, nor to indicate on which data he was relying.

11.32 Our final concern was whether the provision would severely encumber administration. It would affect public sector data users rather than private sector ones and even then only subject to the numerous public interest access exemptions we had proposed. Further, it would only entail the data user advising the individual that a proposed course would be adopted within a specified period unless he brought the data suggesting otherwise to their attention. Such a step would accord with good public administration, although we are not equipped to fully assess all the practical implications. It is possible that the decision-making process may be slowed, but its quality should be enhanced. An alternative approach would be to deal with it as an appeal procedure, but we doubt the practicability of this instead of allowing an input prior to the decision being implemented. For one thing, an administrator might consider that it would entail his admitting that a "wrong" decision had initially been taken.

11.33 We further recommend that "adverse decisions", an expression also used in our matching proposals, be defined.

The nature and aims of data matching

11.34 As mentioned above, "data matching" refers to the process of combining two or more sets of data collected on different occasions but relating to the same individual. The expression is generally used to encompass not only the initial combination of data (including profiling) but also the drawing of inferences and any administrative follow up. Data matching may involve the collation or comparison of data held by different organisations, or within an organisation. Some government departments are large and carry out disparate functions. Similarly, some companies conduct various types of business. In our view matching data held on different databases within an organisation raises the same issues as matching between organisations and our recommendations do not differentiate between these processes.

Investigative matching

11.35 Data matching has a variety of purposes, with a corresponding range of consequences for the data subject. The data matching activity which has elicited the most concern is of an investigative nature. Matching is conducted to identify and investigate apparent discrepancies, or what are referred to as "hits". The comparison process seeks to verify the one set by reference to the other set. What an individual says in one context may be compared with what he says in another. As the main purpose of such matching conducted by the public sector is the protection of the revenue, adverse administrative action may follow, such as the termination of a pension to which the "hit" is no longer thought entitled. The detection of overpayments is similarly a concern of such private sector industries as insurance. It is this form of data matching, referred to as "investigative matching", which is the subject of our specific recommendations set out below.

11.36 Other private sector matching is not investigative in nature. As mentioned in the above discussion of profiling, it may encompass such concerns as identifying bad credit risks or targeting prospective customers more accurately. It may have the completely innocuous aim of reducing duplication of direct marketing lists by consolidating them. This would have the desirable consequence of avoiding multiple copies of the same advertising material being sent to customers. It may even be for the positive purpose of identifying incorrect data and its subsequent correction. Such non-investigative matching which does not involve the identification of discrepancies is subject to the general application of the data protection principles. But it is not the subject of the specific recommendations addressing investigative matching.

Data matching and the data protection principles

11.37 All matching has the potential to infringe the Use Limitation Principle. It will be recalled that this requires that data should not be used for purposes other than those for which they were provided, unless the data

subject's consent is obtained. Data disclosed to one organisation should not be disclosed to another for a different purpose. Similarly, an individual may reasonably expect that data he provides to one section of a large government department shall not be matched and hence disclosed to another section of the same organisation. It is a matter of degree, however, and to the extent that the different sections of an organisation are carrying out the same or similar functions, there will be an expectation by those providing personal data that it will be linked within the organisation. Of course, separate sets of records are not necessary in the absence of functional differentiation within an organisation, precluding the possibility of internal matching.

11.38 If the individual is informed of matching uses at the outset (eg upon applying for a benefit) no contravention of the principles is involved. Such a procedure is known as "front-end verification." But although such matching is not subject to the objections raised by the use of data not announced or anticipated at the time of collection, procedural safeguards may nonetheless be desirable. In particular, it may be appropriate to accord data subjects the right to contest adverse results before administrative action is taken. This issue is considered further below.

Matching and data quality

11.39 The accuracy of a matching program is dependant on:

(i) an accurate identifier;

(ii) accurate data to be matched; and

(iii) valid inferences drawn from the matching.

These factors will now be examined.

11.40 **An accurate identifier** The accuracy of a matching program is dependent on the adequacy of the procedure whereby the individuals referred to in one set of records are inferred to be the same individuals referred to in the comparison set. The simplest and most accurate identifier is a PIN. We have seen that the Hong Kong identity card number is a particularly pervasive PIN, being used in records held for a multiplicity of purposes. In principle, then, it should facilitate accurate inferences that the same individual is being referred to. This is dependant, however, on the number being accurately recorded in each set of records being compared. Experience in Hong Kong indicates that ID card numbers are often incorrectly recorded. A survey conducted at Queen Mary Hospital found an error factor of more than 5%, and Hong Kong Telecom has found the error rate to be 5-10%. Inaccuracy may be partly attributable to the misquoting of the PIN by the individual concerned. Nor need this be inadvertent, particularly if that person has fraudulent designs.

11.41 **Accurate data to be matched** Matching accuracy is also determined by the meaning and quality of the data being matched. The

danger here lies in the ostensible matching of non-comparable items. Relevant factors include:

(i) whether the meaning of key terms such as "income" varies according to context. A graphic example of such variation was provided in para 9.34 above, where only 10-20 out of 1,000 hits were convicted of fraud, primarily because the national law contained 25 different definitions of "income."

(ii) whether "hard" or "soft" data are being compared. This is a continuum ranging from objective facts to subjective opinions. Flaherty gives the example of a person who drinks a quart of spirits a day. That is a "hard" fact, whereas describing that person as an alcoholic is a "soft" fact.

11.42 **Valid inferences** It follows that the matching process may be complex and subject to error. As the range and variability of the data increases, the difficulty in drawing correct inferences increases. Our specific concern is where this process occurs in the context of an investigative matching program. The remainder of this section focuses on investigative matching.

Concerns about investigative matching

11.43 Investigative data matching involving the ostensible match of data to identify "hits" is widely regarded as highly intrusive to privacy interests, particularly when employed in large scale programmes. Individuals identified as "hits" may be subject to adverse decisions without notice, such as the termination of a pension. As accurate matching is dependent on a number of data quality variables, it is dangerous to make such decisions without some form of verification of the matching results. The Australian Privacy Commissioner has characterised investigative matching as "the information society's equivalent of driftnet fishing." The Canadian Privacy Commissioner has likened it to a modern form of search and seizure.

Benefits of investigative matching

11.44 Public sector matching constitutes a checking process on eligibility for benefits, or liability to pay taxes. The detection of fraudulent claims or overpayments assists protection of the revenue and law enforcement. Publicising matching programs may have a deterrent effect on dishonest claims. A similar justification obtains in the private sector credit and insurance industries.

The international control of investigative matching

11.45 Several countries have taken legislative action to regulate investigative data matching. The USA was the first country to do so. Non-statutory guidelines were first released in 1979 and revised in 1982. Legislation followed in 1988. The scope of the Computer Matching and Privacy Protection Act is limited, however. It applies only to matching to verify eligibility for a federal benefit. It requires agencies to enter written agreements concerning their use of matching records. Agencies undertaking matching are also required to set up special boards to oversee compliance with the legal requirements, to conduct cost-benefit analyses, and compile annual reports. In addition, "hits" must be afforded the opportunity to contest the adverse findings.

11.46 Investigative matching has also been addressed in Canada, although by way of policy directives rather than legislation. It is more comprehensive in its scope than the US law, but similarly is restricted to the public sector. It includes the following features:

(i) prior cost-benefit analyses of matching programs, including reference to potential impact on privacy;

(ii) advance notification to Privacy Commissioner;

(iii) approval required by the responsible minister;

(iv) public gazetting of all matching programs; and

(v) verification of adverse findings before taking administrative action.

11.47 Turning from North America to Europe, Sweden's data protection authority has assumed the power to scrutinise and if necessary prohibit data matches. This is notwithstanding the absence of specific legislative reference to matching. The United Kingdom Data Protection Registrar addresses the issue in his latest annual report and concludes that it may now be an appropriate time to regulate matching.

11.48 Perhaps the most comprehensive matching legislation enacted to date is that of Australia. This provides for the issue of detailed public sector guidelines by the Privacy Commissioner. He has subsequently released a set of guidelines with similar features to those contained in the Canadian policy directives described above. His approval is required for all investigative matching programs.

The draft Directive

11.49 Although it does not use the term "investigative data matching", article 18(4) of the revised Directive regulates all processing (defined to

include the alignment or combination of data) where it exposes the data subject to the serious consequences arising from his being identified as a "hit". Article 18(4) provides:

> *"Before Processing which poses specific risks to, the rights and freedoms of individuals commences, the supervisory authority shall examine such processing within a period of 15 days commencing with the date of the notification at the end of which period the authority shall give its conclusions."*

11.50 The Explanatory Memorandum indicates that processing "which poses specific risks" includes but is wider than the processing of the categories of sensitive data such as that relating to political opinions or health. It specifically mentions that it may arise from a processing purpose "which might be to exclude data subjects from an entitlement, a benefit or a contract" (ie the identification of "hits".)

The need for balance

11.51 In view of the above, we view data matching as a procedure which poses a number of data protection dangers and believe that safeguards are warranted when it exposes data subjects to adverse decisions. Not all data matching does so, but when it does controls are in our view desirable. Our specific concern is investigative matching. This is because it combines a matching process, which is generally more susceptible to error than simple profiling, with particularly adverse consequences for data subjects. This greater susceptibility to error resides in the complexity of the matching process. As with profiling of specific data subjects, it requires an accurate identifier. Unlike profiling, however, it further involves complex decisions about the compatibility of ostensibly similar items. Even as regards investigative data matching, however, we recognise that on occasion data protection interests should defer to competing social objectives. We consider that a data protection law should establish a mechanism to balance the different interests. The onus should be on the organisation wishing to conduct a matching program without data subject consent to justify its need.

11.52 While all data matching poses privacy perils, we think it sufficient that the general data protection principles apply to non-investigative matching programs. But **we recommend that supplementary controls are required for investigative data matching involving the comparison of data to identify discrepancies with a view to taking adverse follow-up action against "hits". These supplementary controls are as follows:**

(i) Prior approval of the Privacy Commissioner should be required to all investigative data matching programs, unless all the data subjects included in the program have expressly consented. Such approval may relate only to an individual data user, or it may extend to a sector. The Privacy Commissioner shall promulgate guidelines setting

out the relevant factors in determining whether approval shall be granted. These win include the nature and sensitivity of the personal data, their expected accuracy, and the seriousness of the consequences of being identified as a "hit". Also relevant is whether it is proposed to inform data subjects in advance.

(ii) The guidelines will also set out procedures according "hits" the right to correct matching results before these form the basis for the taking of adverse decisions.

(iii) The onus will be on organisations seeking investigative matching approval to show a competing social need which overrides the privacy interests of data subjects. We envisage that the public sector will more readily discharge this than the private sector. The justification must include an outline of why alternative means of satisfying the objectives are less satisfactory, and a cost/benefit analysis of the program.

Relationship between recommendation on input prior to adverse decision and those on data matching proposals

11.53 The relationship between our recommendation that an opportunity be afforded for input by the data subject prior to the implementation of an adverse decision ("the prior input recommendation") and our data matching recommendations have a common element. Both aim to provide safeguards regarding "adverse decisions". However, they differ in several respects. The matching recommendations deal with programs, whereas the one on prior input encompasses all proposed decisions, including those not arising from a program. The Privacy Commissioner's approval is required for all investigative matching programs to identify discrepancies with a view to follow up action, but not under the prior input recommendation. Approval is required to programs envisaging the identification of "hits", to better ensure the adequate design of the matching process, involving as it does complex inferential processes. This approval is required regardless of whether the application of the program in fact results in the identification of hits. Those identified, however, are to be accorded at that stage the right to correct or supplement matching results in a similar manner to the prior input recommendation.

Submissions on data matching

11.54 A number of comments were received by respondents indicating that we had insufficiently emphasized that our recommendations on data matching solely related to investigative programs for the identification of discrepancies and follow up action adversely affecting the data subject. The above text has been revised in an endeavour to clarify the matter. What we

have in mind is what article 18(4) of the draft Directive refers to as processing which "poses specific risks to the rights and freedoms of individuals". The Explanatory Memorandum gives as examples "processing which has as its object the exclusion of data subjects from a right, a benefit or a contract". It gives as an example of a decision not adversely affecting the data subject the sending of advertising material to a list of persons selected by computer. It follows that data matching engaged in for direct marketing or other comparatively innocuous purposes will not constitute investigative matching and our recommendations on that process will not apply. It is perhaps worth reiterating, however, that the application of the Purpose Specification and Use Limitation principles will preclude matching exercises involving the use of data for purposes not originally specified.

Direct marketing

11.55 The Consultative Document proposed the adoption of article 15(3) of the draft Directive. This provides:

> *"The controller must ensure that the opportunity to have data erased without cost has been expressly offered to a data subject before personal data are disclosed to third parties or used on their behalf for the purposes of marketing by mail."*

11.56 We further proposed that upon the expiration of any appropriate grace period for the law coming into force, data subjects on existing lists who have still not been afforded the opportunity to opt out should be deleted from those lists.

Submissions

11.57 A large number of submissions were received commenting on this requirement. The right of a customer to have the option of having his name removed from marketing lists was not opposed in principle. Indeed, some respondents supported it on both privacy and business grounds. The American Express submission noted that the principle is included in their Privacy Code and commented that:

> *"We cannot overemphasise the importance of opt-out programmes in a balanced privacy approach. In our view, it places the privacy choice on the ones who should decide - the consumers. If consumers choose to receive mail because they like the service then they should receive such items. If a consumer feels his privacy is infringed upon or does not want mailed items, the decision is his or hers not to. It is a situation where everyone, consumers and business, achieve their desired objectives."*

11.58 Nonetheless, a number of direct marketing respondents objected strongly to our proposed mechanism to provide this right. They argued that being required to go through their lists and delete names upon the expiration of the grace period would be time consuming and costly. We accept this. **We therefore recommend that upon the first communication for the purposes of marketing, and at reasonable intervals thereafter, the data subject must be expressly offered the opportunity to have all data relating to him held for marketing purposes erased without cost.**

11.59 This formulation accords (other than the limitation to mailings) with Citibank's suggestion that "the opt out option should be presented to all data subjects during the first direct mailing utilising a compiled data subject listing". Similarly, the ASG Group "recommend that direct mail users be required to print only an 'opt-out' option on all mailing materials". This represents what the Datatrade submission refers to as the "more expensive and less pragmatic" of its two preferred options.

11.60 As direct marketers would not have to go through their lists, we delete as irrelevant reference to a transition period. But the requirement would extend to both pre-existing and new lists to accommodate the inclusion in lists of publicly available data not caught by the principles (see Chapter 15). In choosing an express requirement, we rejected the suggestion that the contact itself constitutes sufficient notice to the data subject. Also, the deletion of reference to marketing "by mail" would broaden its scope to other forms of direct marketing, such as telephone canvassing. We also think it unnecessary to exclude from the scope of the new provision the enclosure of third party material. Express opt-out offers should be offered in relation to every list utilised by the mailer, regardless of whether he is enclosing his own material.

Chapter 12

Data quality and security

Summary

12.1 This chapter looks first at the OECD Data Quality Principle which, in the interests of both the data subject and the data user, requires that data be relevant, accurate, up-to-date, and complete. Where the data user discovers that he has transferred incorrect data, he should notify recipients of corrections.

12.2 Incorrect data can arise through inadvertent computer error, technical failure, or intentional misuse. Intentional misuse, and in particular unauthorised access (popularly known as "hacking"), has received considerable public attention.

12.3 The second part of the chapter looks at the OECD Security Safeguards Principle which requires the adoption of reasonable security safeguards to protect data from all risks to its integrity. These safeguards should include not only technical measures but also appropriate management functions. As the evidence indicates that computer operating error is the principal cause of defective data, this will include adequate training and procedures. We conclude that security safeguards should apply to both automated and manual data.

Recommendations

12.4 Personal data should be kept accurate and, where necessary, up to date. A breach of the accuracy requirement is compensatable for loss caused. Compensation is not payable where the data accurately records information received from a data subject or third party and the data are identified as such (paragraph 12.12), or where the inaccuracy occurs despite all reasonably practicable steps being taken (paragraph 12.13).

12.5 Data which are inaccurate or incomplete having regard to the purpose for which they are held, should be erased or rectified. Data should not be kept in a form which permits identification of the data subject any longer than is necessary for the fulfilment of the data purposes (paragraph 12.15).

12.6 Data users should be subject to the duty to take such reasonably practicable steps as are necessary to correct data transferred, having regard to the nature and effect of the data (paragraph 12.16).

12.7 Data users should be required to take all reasonably appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of, both automated and manually stored personal data and against accidental loss or destruction of such data. In determining the scope of this duty, regard shall be had to:

(a) the nature of the personal data and the harm that would result from such access, alteration, disclosure, loss or destruction as are mentioned in this principle; and

(b) the place where the personal data are stored, to security measures programmed into the relevant equipment and to measures taken for ensuring the reliability of staff having access to the data (paragraph 12.33).

OECD Data Quality Principle

12.8 This provides as follows:

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

12.9 We recommend that to comply with this principle data must be:

(i) *relevant* to the data purposes. This was dealt with in relation to the collection phase in Chapter 9. But the requirement is not restricted to this phase. It follows that if purposes alter and data cease to be relevant, they should be deleted.

(ii) *accurate* so as to adequately reflect the real world. Accuracy is related to the precision of data. The precision required of data will depend on the purpose. The need for precise age data, for example, will be less in a survey only seeking to place respondents in age bands (26-35, for example) than other uses such as medical records.

(iii) *up-to-date* so that the data reflect the present position. This is subject to any statutory requirement that the data be retained for a specified period.

(iv) *complete*. This refers to the requirement that there be sufficient data to avoid the drawing of false inferences. It is to be distinguished from "comprehensive", which would require the compilation of all available data. False inferences may also be drawn due to insufficient attention to context.

Scale of the problem

12.10 We have already made passing reference to studies documenting inaccuracies in personal data. In Chapter 1 a US study was cited where the percentage of state criminal history records found to be complete, accurate and unambiguous ranged from 49.5% down to a mere 12.2%. In Chapter 9 reference was made to a Swedish data matching exercise which illustrated the scope for false inferences arising from insufficient attention to context. Of approximately 1,000 persons identified as defrauding the social security system, only 10-20 were convicted. The explanation for the misleading matching results lay in the 25 different definitions of "income" used in the files matched.

UK Data Protection Act

12.11 This enactment puts the accuracy requirement succinctly. The 5th principle states:

> *"Personal data shall be accurate and, where necessary, kept up to date."*

12.12 Section 22 of the same Act provides a right to compensation to data subjects who suffer damage "by reason of the inaccuracy of the data." This does not, however, extend to accurate records of data received from a data subject or third party and identified as such. As the Registrar has observed, lack of such a qualification would effectively require data users to guarantee the accuracy of what they were told by others.[1] But if this approach is adopted, consideration must be given to a requirement that data users notify third parties of corrections to data which the data users have previously communicated to them. This is dealt with below. Subject to this, **we recommend adoption of a legal requirement that personal data be kept accurate and, where necessary, up to date.** Regarding compensation, in Chapter 16 we recommend a general right to compensation for a breach of the legal provisions of the data protection law causing loss (Chapter 8 recommends that compensation shall not be payable during an initial transition period). **We further recommend (along the lines of the UK legislation), however, that a breach of the accuracy requirement is not compensatable where the data accurately records information received from a data subject or third party and the data are identified as such.**

Submissions

12.13 Concern was expressed to us by, *inter alia*, Citibank and the Hong Kong Housing Authority about our proposal that a data user be absolutely liable to pay compensation for inaccurate data, with no defence that all reasonable care was taken. As was pointed out, 100% accuracy of

---

1 Fifth Report of the Data Protection Registrar, June 1989, London: HMSO, 1989.

inputting cannot be guaranteed. **We accordingly recommend that there should be no liability for compensation provided all reasonably practicable steps had been taken to ensure the accuracy of data held.** The duty would be higher for data with a higher risk to the data subject. Sectoral codes would be able to flesh out the content of the duty and compliance would avoid liability. We also addressed the question of whether the data subject should have a legal duty to assist the data user to maintain accurate data. For example, members of Government Committees are provided a print-out annually of the personal details held in relation to them. More generally, should an individual who wins the Mark Six (or goes bankrupt) notify his bank? The basic principle should be that the individual should not benefit from his own wrongdoing. The analogous legal concept is that of contributory negligence. Companies could place a legal onus in the contract. Failing this, however, we decline to impose a specific legal duty on the individual to accurately maintain data relating to him. To do so could result in a flood of access requests. Such omissions would simply be a relevant matter in determining whether the data user had taken all reasonably practicable steps.

Duty to maintain accurate records

12.14 Data quality is not a static attribute and so the duty to maintain data quality is a continuing obligation. Often record keepers will be assisted in this regard by data subjects availing themselves of their access and correction rights as discussed in chapter 14. The Data Quality Principle, however, clearly places the onus on data users to take the necessary steps to maintain data quality. Data subject correction rights supplement this obligation; they do not qualify it.

Remedying inaccurate records

12.15 The OECD Guidelines do not specifically require the destruction of out-of-date records. The accompanying Explanatory Memorandum, however, recommends the erasure or anonymisation of data no longer serving a purpose. The draft Directive is more explicit. Article 6 specifically adverts to the matter. It requires that data which are inaccurate or incomplete having regard to the purpose for which they are held be erased or rectified. It further provides that data should not be kept in a form which permits identification of the data subject any longer than is necessary for the fulfilment of the data purpose. **We recommend that these requirements be included in the Hong Kong law.** This is subject to two points. Firstly, erasure of automated data is technically difficult and for the purposes of our recommendation "erasure" means "removed from the system so that it cannot be retrieved by ordinary means". The second point, which is made by the draft Directive, is that archival, statistical and scientific records require separate consideration. Such records raise considerations beyond those of the protection of personal data and, with the exception of an exemption for

research data discussed at chapter 15, we have not attempted to deal with them.

Duty to notify third parties of corrections

12.16 In Chapter 10 we dealt with the disclosure of personal data. The situation will often arise where a data user has disseminated data that subsequently requires correction or updating. Unless the data are corrected not only by the original transferor, but also by the transferees, the data subject's interests may be severely affected. Indeed, the transferees' interests will also be prejudiced, as they will making decisions on the basis of defective data. We have accordingly considered whether a legal duty should be imposed on those transferring data to ensure that corrections are passed on. One method would be to maintain audit trails on all disseminated data. We consider this an unduly onerous duty to impose in all cases. Nor would such tagging of data be the only possible method of checking where data had been transferred to. For example, if the transferor only discloses data on a regular basis to a limited list of transferees, then he could simply propagate all updates to those listed, on the basis of an agreement that they apply the updates. Another possibility for credit checks would be to notify a central agency for distribution of corrections as required. In short, it would not be necessary to stipulate the method of propagating corrections. It would be a matter for the data user to devise an adequate system. On this basis **we recommend imposing on the data user the duty to take such reasonably practicable steps as are necessary to correct data transferred, having regard to the nature and effect of the data.** This formulation accommodates the sensitivity of the data, as the more sensitive it is (eg HIV status) the more vital that it be corrected. This is likely to be facilitated by the tendency to progressively restrict the dissemination of data as its sensitivity increases. While we recognise that this duty may sometimes be onerous, we consider that if a data user chooses to transfer data, the onus should be on him to update that data. The duty is distinct from and additional to the duty arising under the Use Limitation Principle discussed in the previous chapter.

Data quality and good information practices

12.17 The Data Quality Principle is essentially a rule of good information and records management. It is not in the interests of data users to make erroneous decisions on the basis of irrelevant or inaccurate data. This is quite apart from the adverse consequences incurred by the data subject.

OECD Security Safeguards Principle

12.18 This provides as follows:

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

It will be observed that this principle sets out by way of examples a number of specific risks regarding personal data which should be guarded against. In view of our recommendation that non-automated as well as automated records should be regulated, safeguards for both computers and hardcopies will be required. Paper files can be kept under lock and key. The security of computer programs can be achieved by making access user specific or terminal specific. Software applications achieve a similar result through the scrambling of signals, known as encryption, so that they are unintelligible until unscrambled.

The relativity of data security

12.19 Data security is a matter of degree. This is particularly so regarding automated records. As one expert puts it:

> *"Absolute security is unattainable. No matter how good the protective measures, there will always be some means of damaging the computer or data. The objective of any review of security is to minimise the exposure that a company faces. There are a large number of techniques available to enhance security and not all will be useful or applicable in any particular organisation. It is necessary to select those that give the best value."*[2]

Data security and personal computers

12.20 A whole new dimension to data security has been created by the proliferation of microcomputers, including personal computers. The general implications of microcomputers were summarised in Chapter 1. Microcomputers may be linked together into communications networks. The portable nature of microcomputers makes it impracticable to require that they be kept in segregated areas with restricted access. In theory, the greater difficulties encountered in effectively limiting physical access to microcomputers may be combatted by restricting operational access through logic or software controls. But even password control, regarded as only an initial aid to computer security, is seldom incorporated in microcomputers.[3] Microcomputers are also operated in a technically casual environment by individuals with different levels of training. Operating errors adversely affecting data quality are accordingly a distinct risk. These include such problems as accidental erasure which are not addressed by encryption.

---

2 D. Bradburn, "An Introduction to Tata Security" in Hearnden (ed.), *A Handbook of Computer Security* (London: Kogan Page, Revised edn; 1990), page 25.

3 K. Hearnden, "Microcomputer Security" in Hearnden, *ibid*, page 150.

12.21 Data security risks can for convenience be put into three categories: intentional computer misuse, computer error, and technical failures. The first two categories are caused by individuals and are now discussed.

12.22 **Intentional computer misuse** The destruction of data on a vast scale can result from the introduction of viruses through the unauthorised accessing of computer networks by outsiders. Estimates of the annual cost of computer abuse to British industry have ranged from £200 million pounds to £1.5 billion.[4]

12.23 Viruses causing widespread dislocation and loss have attracted media attention and generated public concern. But:

> *"all the evidence suggests that the substantial majority of computer-linked crime is carried out by employees attacking the integrity of their own organisation's computers."*[5]

12.24 The Computer Crimes Ordinance 1993 effected several amendments to existing laws to counter computer misuse. Of particular relevance to the present discussion are sections 2, 3 and 5. Section 3 extends the offence of criminal damage to:

(a) causing a computer not to function normally;

(b) altering or erasing any computer program or data; and

(c) adding any program to a computer.

12.25 A conviction under this provision carries a maximum penalty of 10 years imprisonment. Section 2 addresses the problem of unauthorised access by means of remote means, usually a personal computer or a modem and telephone. It is popularly referred to as "hacking". Section 2 creates the new offence of unauthorised access to a computer by "telecommunication" (i.e. remote means). The maximum penalty is a fine of $20,000.

12.26 The proposed new offence of unauthorised access does not require any proof that it was done with the intent to gain, or to cause loss to another. Mere curiosity or the desire to "beat the system" can suffice. So too, however, will prying into another's personal data. The requirement that the Attorney General consent to a prosecution is intended to screen out innocuous instances.

12.27 Access for gain is dealt with by section 5. This makes it an offence for a person to obtain access to a computer-

(a) with intent to commit an offence;

---

4 K. Hearnden, '"Computer Security" in Hearnden, *ibid*, page 4.

5 Hearnden, *ibid,* page 5.

(b) with a dishonest intent to deceive;

(c) with a view to dishonest gain for himself or another; or

(d) with a dishonest intent to cause loss to another.

12.28 This offence carries a maximum penalty of 5 years imprisonment. It will provide a valuable weapon to combat the unauthorised sale of personal data. This is an increasing problem. The New South Wales experience is discussed in Chapter 5. A further example is provided by a recently completed US federal investigation of the alleged nation-wide bribery of Social Security Administration employees to conduct computer searches of thousands of data subjects. The officials would receive US$25 per individual from "information brokers" who would sell each data subject's details for US$175 to private investigators, creditors and businesses.

12.29 **Computer operating error** The intentional misuse of computers poses significant security risks to the integrity of personal data. The criminal sanctions contained in the Computer Crimes Ordinance are aimed at deterring such conduct. But another major area of risk to data quality is posed by inadvertent operator error. In the view of one expert "... accidental damage to computers, their operating systems and data almost certainly accounts for more incidents than deliberate actions taken against them."[6] Obviously, criminal deterrents would be both an inappropriate and an ineffective method of dealing with this problem. Instead a partial answer lies in adequate training and procedures.

Legal provision for data security

12.30 Article 17 of the ECC draft Directive states:

> *"Member States shall provide that the controller must take appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss and against unauthorised alteration or disclosure or any other unauthorized form of processing. Such measures shall ensure, in respect of the automated processing of data, a suitable level of security having regard to the state of the art and the nature of the data to be protected, and an evaluation of the potential risks involved."*

12.31 The UK Data Protection Act is along similar lines. The eighth principle states:

> *"Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction*

[6] D. Hearnden, "Computer Linked Crime" in Hearnden, *op cit*, page 11.

of, personal data and against accidental loss or destruction of personal data."

12.32 The relevant interpretation clause states:

"Regard shall be had-

(a) to the nature of the personal data and the harm that would result from such access, alteration, disclosure, loss or destruction as are mentioned in this principle; and

(b) to the place where the personal data are stored, to security measures programmed into the relevant equipment and to measures taken for ensuring the reliability of staff having access to the data."

12.33 We prefer the UK formulation for its clarity, although we would insert "reasonably" before "appropriate security measures." It would also have to be made clear that the provision extends to all records, as was explained in Chapter 8. Subject to this, **we recommend its adoption.**

12.34 The two provisions are similar in that they do not attempt to tie measures to a particular state of technology. This is also the approach taken by other data protection laws and coincides with our own. We also agree that it is impracticable to stipulate a detailed set of data security requirements for all data users. When carrying out his investigations, it will be a question of fact for the Privacy Commissioner to determine whether there has been compliance in all the circumstances. The UK provision explicitly recognises that data security is very much a staff management function and not merely a technical problem.

Submissions

12.35 A number of submissions asked for more detailed guidance than that provided by the above formulation. Upon further consideration, however, we confirm our earlier view and decline to provide more explicit general guidance. We note that this was the approach adopted by the OECD in its recent review of the issue.[7] It concludes :

"While seeking harmonized standards, it should be recalled that, as to individual situations, there can be no one security solution. Security needs vary considerably from sector to sector, company to company, department to department, and, as to given information systems, over time. Lack of an informed and balanced understanding of users' needs may create a significant risk of "off-target" technology standardisation. A productive first

[7] Guidelines for the Security of Information Systems Organisation for Economic Co-operation and Development Paris 1992, page 31.

step is recognition of the inherent diversity and heterogeneity of users' needs for information system safeguards."

12.36 It follows that the best place for more detailed guidance on data security is in the sectoral codes.

Chapter 13

Openness and data protection

Summary

13.1 The OECD openness principle has both general and specific aspects. The former requires that the public be advised of the nature and scope of record systems to promote the scrutiny of administrative and technological developments affecting data protection. The latter stipulates that means must be available for an individual to ascertain whether data is held concerning him. We concluded in Chapter 10 that this could be achieved by a requirement that the data user furnish the data protection authority with a declaration describing his data purposes.

13.2 We develop that proposal in this chapter. Our aim is to restrict the contents of declarations to the bare essentials. The vast majority of personal data users are small businesses engaged in a limited number of common data purposes. To facilitate completion, we think that the declaration for mainstream data purposes should be in a multiple-choice format. As public sector declarations should be more comprehensive, they will not be susceptible to a multi-choice format.

13.3 We consider easy access to the contents of declarations by interested individuals is essential if data subjects are to be able to effectively exercise their rights of data access and correction.

Recommendations

13.4 There should be a statutory policy of openness about developments, practices and policies with respect to personal data. This principle should be taken into account:

(i) by the Privacy Commissioner in the carrying out of his functions;

(ii) by the Administrative Appeals Board and the courts; and

(iii) in the formulation and approval of sectoral codes (paragraph 13.19).

13.5 Public sector users of personal data should compile declarations describing the following features of a personal records system:

(i) the purposes for which the data are kept;

(ii) the content of data contained in the classes of record, including any sensitive content, namely data revealing racial or ethnic origin, political opinions, religious beliefs, philosophical or ethical persuasion or trade union membership, and of data concerning health or sexual life;

(iii) the classes of individuals about whom records are kept;

(iv) to whom the data are usually disclosed;

(v) the functional title and contact details of the individual (the responsible officer) who can provide information to data subjects about access to their personal data; and

(vi) countries to which personal data are exported (paragraph 13.22).

13.6 Private sector data users should compile declarations identifying all data purposes and the contact details of the responsible officer (paragraph 13.25). The Privacy Commissioner should be empowered to prescribe the forms to be used in making declarations (paragraph 13.39).

13.7 Although a data user is only required to lodge one declaration, separate entries should be made for each distinct data purpose (paragraph 13.30).

13.8 For mainstream small business users the declaration will take the form of a structured multi-choice questionnaire. This will accommodate a small number of data purposes which are commonly engaged in (paragraph 13.29).

13.9 A system should be established to provide interested individuals with on-line access to the contents of declarations of organisations (paragraph 13.37).

13.10 Every data user should designate a responsible officer to facilitate compliance. The officer may be jointly liable with the organisation for a breach of the data protection principles (paragraph 13.41).

OECD Openness Principle

13.11 The OECD Openness Principle provides:

> *"There should be a general policy of openness about developments, practices 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."*

A general policy of openness

13.12 The function of the "general policy of openness about developments, practices and policies" so far as data subjects are concerned is that:

> *"if they consider features of them to be undesirable or dangerous, they can seek, through the appropriate legal or (more likely) political channels, to have controls imposed."*[1]

Openness about new developments

13.13 Openness about developments impinging on data protection is necessary to avoid a constant process of accommodating insidious administrative and technological initiatives. The point is made by Flaherty in his review of the operation of data protection laws.[2] Overseas experience has demonstrated the following:

(i) the difficulty of reorganising administrative processes once they have been established. In recognition of this the German Data Protection Commission exercises an advisory or "preventative" role in encouraging the inclusion of data protection provisions in other legislation and regulations.

(ii) the importance of developing a system of early consultation on privacy implications of new technology. Flaherty cites the cautionary example of the French data protection authority's response to a new development. That authority is tasked generally to consider the problems posed by information technology. The agency announced its interest in the development of expert systems at an early stage, but waited until such a system became operational before scrutinising the issue. Flaherty comments that post-implementation examination of new systems involving major investment precludes effective input, inhibiting the introduction of protective modifications. Our concern is not limited to new technology, however. New applications of existing technology or administrative procedures may have even greater impact on data processing. Examples are the standardisation of equipment and definitions to facilitate investigative data matching.

13.14 Both (i) and (ii) involve supervisory authorities in the assessment of what the Openness Principle refers to as a concern with "developments, practices and policies with respect to personal data". We discuss the

---

1 Roger Clarke, *OECD Guidelines: A Template for Evaluating Information Privacy Law and Proposals for Information Privacy Law* (1988 Xamax Consultancy P/L)

2 David Flaherty, *op cit*, page 30.

recommended functions and powers of a data protection agency in Chapter 16.

Legal content of the Openness Principle

13.15 The very generality of the "general policy of openness" makes it difficult to give legal content to the principle other than by attributing the relevant function to an oversight authority. This may explain why many laws based around the data protection principles do not specifically advert to it, although specific provisions may reflect it. Neither the UK Data Protection Act nor the Australian Privacy Act count it amongst their statutory guidelines (the latter, however, does confer on the Privacy Commissioner the function of monitoring developments in data processing). Nor does the draft Directive refer to it. An example of a recommendation with more specific objectives which will also enhance openness is that investigative data matching be controlled by guidelines. Those guidelines will provide for public notification of matching programmes.

13.16 The uncertain application of the Openness Principle is largely attributable to its failure to identify who is responsible for its implementation. The other principles discussed in this document clearly impose duties on record keepers regarding the collection, use and safekeeping of data. These duties relate to the every-day operations of data users. The focus of the Openness Principle, however, extends beyond this to encompass more general concerns which are not specific to particular data users, but shared by many. New technologies, legal regulations, and sectoral requirements are examples. In this situation it is more difficult to attempt to fix a legal duty on individual data users.

13.17 The difficulties are compounded by attempting to identify the contents of the duty. Should it, for example, extend to a duty of notification of a novel technology or new practice? If so, should the duty arise at the planning or implementation stage? And should data subjects be notified, or only the data protection authority?

13.18 In view of the above, there appear to be at least four possible approaches to the requirement of openness about policies, practices and policies:

(i) to retain the principle in its present general form. As such it would represent a broad exhortation not giving rise to any specific duties;

(ii) to omit the principle from the set of statutory guidelines;

(iii) to impose a duty on individual data users to discharge the requirement. This could be done by requiring the matter to be canvassed in the declarations they are required to compile describing their personal data. Other jurisdictions requiring

declarations restrict the items needing description to such matters as the purposes for which records are kept and the classes of individuals recorded. It would be possible, however, to also require the description of any new practices, policies, or technologies; or

(iv) to impose a duty, but on sectors and not individual data users.

13.19 **We recommend that the duty should not be directly imposed on individual data users. We do not, for example, think it would be practical to require that declarations refer to new administrative or technological developments. The broad principle should be included in the statutory guidelines, as it emphasises that the public should be consulted in the formulation of policies on personal data. They should not be developed "in a huddle". To this extent, the principle represents a weak freedom of information requirement. The principle should be taken into account by the Privacy Commissioner in carrying out his functions. Similarly, the Administrative Appeals Board and the courts should have regard to it. Last but not least, it should be taken into account in the formulation and approval of sectoral codes.** We note that the Netherlands law usefully addresses this last aspect. It provides that in determining whether the code complies with the law, the data protection authority shall take into account whether it was prepared by those sufficiently representative of the sector and whether there was sufficient consultation with those affected, including data subjects.

Means to establish existence of personal data

13.20 The more specific concern of the principle is that mechanisms should exist to facilitate individual data subjects ascertaining what data are held which pertains to them. As appears from the Explanatory Memorandum, the OECD considered this a prerequisite to the exercise of the access and correction rights conferred by the Individual Participation Principle discussed in the next chapter.

The role of declarations

13.21 Whilst there may be difficulties in imposing a legal duty on data users to disclose new practices, policies and technologies, it is a simpler matter to provide means of establishing the existence and nature of personal data. In Chapter 10 we recommended that there should be a legal requirement that data users compile a declaration briefly describing their record systems, including a specification of the purposes for which information is held. This recommendation was made in the context of ensuring that personal data shall only be held for specified purposes, as required by the Purpose Specification Principle. Adoption of this recommendation would, however, fulfil the further function of facilitating data subjects ascertaining the existence of data relating to them, particularly when it is coupled with the

ancillary recommendation that a copy of the declaration be furnished to a central authority. The remainder of this chapter discusses appropriate supplementary mechanisms to effect this.

Contents of public sector declarations

13.22 In order to discharge adequately the requirements of both the Purpose Specification Principle and the Openness Principle, **we recommend that declarations of public sector data users describe the following features of a personal records system:**

(a) the purposes for which the data are kept;

(b) the content of data contained in the classes of record, including any sensitive content as defined by article 8 of the draft Directive (i.e. data revealing racial or ethnic origin, political opinions, religious beliefs, philosophical or ethical persuasion or trade union membership, and of data concerning health or sexual life);

(c) the classes of individuals about whom records are kept. This would *not* entail the identification of data subjects;

(d) to whom the data are usually disclosed;

(e) the functional title and contact details of the person (the responsible officer) who can provide information to data subjects about access to their personal data; and

(f) countries to which personal data are exported.

13.23 Australia requires its government departments to furnish declarations covering all the items we have listed. A perusal of the 1989 digest compilation of declaration entries shows that each of the above items can usually be disposed of in one sentence and entries run to a total average length of some 250 words. Specimen declarations are contained at Appendix 4. It lists only one entry for personal records held by the Australian Institute of Criminology, namely personnel records. But 201 entries are included in the declaration of the Australian Federal Police. They cover such diverse matters as aliases, breathalyser records, extremist groups, interpreter services, lost property, missing persons, payrolls, and VIP protection. Obviously, the descriptions of the items we have identified will differ in each case. We recognise that compiling a list of all data purposes will require government departments to crystallise them, perhaps for the first time. This will be a major initial task but is nonetheless essential. An entry which attempted to describe the data subjects of both terrorist and interpreter files would be both confused and confusing. A separate entry for each distinct purpose, however, facilitates both clarity and brevity in its compilation and interpretation.

Furthermore, once identified, there is likely to be little need to subsequently amend the entries.

Contents of private sector declarations

13.24 The Consultative Document proposed that private sector declarations cover all the matters (i.e. (a) - (f) of paragraph 13.22) we recommend be described in public sector declarations. However, public consultation elicited a number of submissions. One submission queried the requirement on the basis that in itself it would not ensure compliance and would engage resources in obtaining and updating the information. It was suggested by the Coalition of Services Industries that the benefit to the data user would be outweighed by the administrative burden of compilation and the significant expenses involved in setting up and maintaining an up-to-date records system. Several overseas experts mention that the system may be perceived as having a "Big Brother" aspect. Other submissions do not challenge such a requirement, but emphasise that it should stick to essentials.

13.25 In view of these concerns, we considered whether it was essential for organisations to specify all the matters we had originally proposed. We concluded that this was the case in the public sector. We came to the view that a rudimentary declaration system was also fundamental to our regulatory scheme for the private sector. The single most vital function of declarations is to identify data purposes. This was essential for the application of the Purpose Specification Principle. It was also necessary to enable the data subject and the Privacy Commissioner to check compliance with the principle. Otherwise, organisations would be able to redefine their data purposes as expediency required, and to retrospectively legitimate the use of data contrary to the data subject's expectations. The other essential item was the designation of the Responsible Officer, to facilitate contact. **We therefore recommend that private sector declarations identify all data purposes and include contact details of the responsible officer.** The remaining items we had originally thought should be covered in all declarations were:

(i) the content of data contained in the classes of record, including any sensitive content;

(ii) the classes of individuals about whom records are kept;

(iii) to whom data are usually disclosed; and

(iv) countries to which personal data are exported to.

13.26 We have concluded that whilst inclusion of these items would be useful, we do not recommend their inclusion at this stage but think that this should be kept under review by the Privacy Commissioner. Their retention for private sector organisations was not absolutely essential. Public sector organisations, however, would not be using the declaration form tied to the

business registration system and should be required to describe briefly these other matters. This is one area where we think that differentiating between the two sectors is justified. We note that a particular concern of the Legislative Council Panel on Information Policy is that individuals be able to ascertain whether public authorities hold sensitive data on them. The more comprehensive declaration form requires that this be specified.

13.27 The simplified business registration/declaration details should largely answer the concerns of respondents. Nor would it usually require updating. The corollary of the lessened "Big Brother" element was that the Privacy Commissioner would become more dependent on complaints to identify data trends. He would still be able to require further and better particulars when necessary.

Multi-choice questionnaire declarations for businesses

13.28 The UK Data Protection Act requires both public and private sector data users to lodge declarations. Most of those lodging declarations are small businesses and a simplified form has been prepared for them. The form accommodates only the four most common record-keeping purposes: personnel administration, marketing/selling, purchasing, and customer/client administration. To facilitate completion of the declaration, it has been structured as a multiple-choice questionnaire requiring the ticking of appropriate boxes. 24 different classes of data are listed as examples. Data users are not confined to the boxes.

13.29 Such a structured form of declaration is neither feasible nor even desirable with large multi-purpose public and private sector organisations. But we see definite advantages in the UK approach as regards businesses with limited record keeping purposes. It provides some precision in the specification of purposes and the description of the associated activities. This is preferable to leaving it to those completing the declaration to create their own formulations. The more structured format should also serve to orientate those completing the declaration. Small businesses are less likely to possess the resources and expertise in this regard which are available to larger organisations. The resultant precision should also assist in protecting the interests of the data subject. That said, however, we must add that we consider the format of the UK small business declaration is far too complex in the Hong Kong context. This is because it attempts to cover all uses. We understand that the form has not been used much, as most data users have a core use and a supplementary one. Our preferred approach is to attempt only to accommodate the 90% of mainstream users. **We therefore recommend the adoption of a structured multi-choice questionnaire format for small business declarations, but covering a much more restricted range of data purposes than the UK format.** We attach at Appendix 5 a proposed draft form.

Separate entries for each file/database

13.30 Whilst most organisations pursue only one or two functions or activities, others will pursue many. **Each different activity will require a separate set of records held for disparate purposes. It follows that although a data user is only required to lodge one declaration, separate entries should be made for each separate data purpose and we so recommend.**

13.31 This recommendation deletes the Consultative Document's reference to "functionally separate databases". We agree with several respondents that data purposes are the relevant consideration, rather than "functionally separate" data bases. The latter concept is a difficult one, and in any event the linkage of data bases is an ongoing matter subject to constant alteration. The essential point is the use to which the data is put, and working backwards from the description of this would facilitate assessment of the legitimacy of the collection of the data. Data holders are changing their emphasis and increasingly retrieve their data on the basis of the purpose for which it will be used. Data subjects will be able to identify the data purposes they are interested in and request access to those specific categories.

13.32 The same point is made in slightly different language by the draft Directive. Article 18 requires a separate notification for every data processing operation "intended to serve a single purpose or several related purposes." The Explanatory Memorandum elaborates that this accommodates:

> *"… several purposes which are related between themselves from the point of view of the controller and of the data subject. By way of example, a single notification would be required for all the processing operations concerning the management of loans given by a credit institution: this might include registering the application, investigating it, approving it, recovering debts due and keeping track of legal proceedings."*

Public access to declarations

13.33 An important function of declarations is that they be public documents. The Openness Principle requires that means should be readily available of establishing the existence and nature of personal data. As the OECD Explanatory Memorandum explains, "readily available" implies that individuals should be able to obtain information with only reasonable effort as to time, advance knowledge, travelling, and cost.

13.34 We recommend in Chapter 10 that data users furnish a central authority with a copy of their declaration. It is envisaged that this agency will be computerised and this will enable individuals to obtain access by keying in the name of the organisation in question. This would be feasible from both private terminals and public terminals especially provided for the purpose.

Details of the declarations which are accessed would be projected onto a screen. Printouts would also be possible. We note that in the USA the facility already exists whereby a fax is elicited by dialling the relevant telephone code number.

Indexes of declarations

13.35 Additionally or alternatively to this on-line approach, other jurisdictions have compiled printed indexes of all declarations. We have already mentioned the Australian Personal Information Digest. Whilst these may be useful in more physically dispersed jurisdictions, we do not consider they would serve any useful function in Hong Kong. We note also that many commentators doubt the utility of such printed indexes. Flaherty's review of their operation[3] indicates that they are little used in France and the US, although slightly more so in Canada. Despite its registration system, Sweden does not attempt to publish a central register. Instead it publishes a small booklet which includes reference to the most important entries.

13.36 We find the UK experience instructive in this regard. A central register has been compiled but the Registrar considers that the register "provides only limited help in directing an individual to where information about him or her might be held."[4] This is confirmed by the Home Office Review.[5] Flaherty points out that a problem with digests and central registers which are printed and hence not on-line is that of keeping them up to date.

13.37 **In view of the above, we recommend a system providing interested individuals with on-line access to the contents of declarations of organisations.** We believe such a system will satisfy the OECD requirement that means are "readily available" to enable data subjects to establish the existence and nature of personal data. The next chapter describes supplementary mechanisms to achieve this, namely data subject access and correction rights.

Notification of data subjects

13.38 The above recommendation requires the individual to take the initiative in ascertaining the contents of declarations. Whilst declarations are public documents of potential interest to community members generally, usually an individual will be concerned to examine the declaration of organisations he suspects hold personal data on him. It follows that the aims of the Openness Principle would be better served by imposing a duty on data users to notify an individual whenever it holds personal data on him. This issue was discussed above in Chapter 10. We concluded that the combined effect of the collection and declaration requirements was to provide a

---

3 David Flaherty, *op cit,* page 30.

4 Fifth Report of the Data Protection Registrar, June 1989, London: HMSO, 1989.

5 Home Office, *Review of the Data Protection Act: Report on Structure*, HMSO, 1990.

sufficient degree of transparency without such a notification requirement that data subjects be notified when data relating to them is first stored.

Form of declaration

13.39 We have discussed in some detail the information which should be contained in the declarations to be submitted to the Privacy Commissioner. We do not think, however, that the form itself should be included in the legislation. It should be left to the Privacy Commissioner to prescribe the forms which are to be used. This approach will provide greater flexibility and allow the Privacy Commissioner to respond to changing needs as they arise, without the necessity of resorting to the complications of amending legislation. **We accordingly recommend that the Privacy Commissioner be empowered to prescribe the forms to be used in making declarations.**

Appointment of Responsible Officer

13.40 We consider it essential that data users designate an officer (ie necessarily a natural person) to coordinate compliance with the organisation's data protection duties. The designation of a specific officer to respond to access requests, monitor data security arrangements and so forth should have a beneficial effect on standards. It is also important that the public has a specific contact point. Other jurisdictions such as Canada and Australia have found such an arrangement to be invaluable in the public sector. We accordingly recommend that every data user designate a responsible officer to facilitate compliance with the law. We have recommended above that the contact details of the responsible individual should also be included in the declaration. We have specified this as a functional title rather than an individual's name in order to accommodate personnel changes and reduce the need for updating.

13.41 Several respondents sought clarification of the responsible officer's role and responsibilities. We envisage that he would perform the functions of monitoring compliance, training staff, and liaising with data subjects. He would require a rank commensurate with these functions. We considered whether the responsible officer should be liable for any breach of the data protection principles. This would encourage the responsible officer to be diligent in the exercise of his duties but could prove unfair where the faults penalised were those of the system rather than the officer himself. **We intend, however, that liability should not attach to the responsible officer merely by virtue of his status, but that some personal culpability would need to be demonstrated. Subject to that, we recommend that the responsible officer may be jointly liable with the organisation for any breach of the data protection law.** We examine in Chapter 16 what infractions will amount to criminal offences under the new law.

Chapter 14

Data subjects' rights of access and correction

Summary

14.1 This chapter examines the OECD Individual Participation principle. Unlike the other OECD principles, which impose duties on data users for the protection of data subjects, the Individual Participation Principle confers specific rights on data subjects.

14.2 This principle gives data subjects access and correction rights. These rights are fundamental to the operation of an effective scheme to regulate the use of personal data and are described in the OECD Explanatory Memorandum as "perhaps the most important privacy protection". We conclude that it is not feasible for a data protection authority to have the exclusive role of monitoring compliance and it is essential to involve data subjects in the process if it is to be effective.

Recommendations

14.3 Access and correction rights should not be restricted to Hong Kong residents (paragraph 14.19).

14.4 An interested individual should be legally entitled to be informed by a data user whether the latter's data refer to that individual; and if so, to be supplied with a copy of that data (paragraph 14.22).

14.5 Upon receipt of an inquiry as to whether data exist which is unaccompanied by a request for such data, the data user should have a discretion as to whether to provide a copy of that data at that stage, or to await a specific request for a copy (paragraph 14.22).

14.6 A nominal, waivable, fee should be payable by a data subject for inquiring as to whether data exist relating to him. A nominal (not cost-related) fee should be payable for full access requests which require the supply of a copy of data held, to deter mischievous requests. It should operate as a maximum, and organisations should be at liberty to reduce or even waive it (paragraph 14.26). A fee may be charged on a commercial basis if a copy had been provided earlier (paragraph 14.28).

14.7 Access fees should be provided for in subsidiary legislation and in a manner facilitating their updating as required (paragraph 14.31).

14.8 Data access requests should be in a recorded form, although data users may waive this requirement and accept requests by terminals or telephone (paragraph 14.32).

14.9 Data provided in response to access requests should be in an intelligible form, unless they are contained in a true copy of a written document which is unintelligible on its face. Data should be supplied in the language in which it is held and where data is held in more than one language, it should be provided in both languages (paragraph 14.33).

14.10 Access requests should be complied with within 45 days (paragraph 14.36).

14.11 A data user should not be required to respond to subject access requests:

(a) unless he is supplied with such information as he may reasonably require in order to satisfy himself as to the identity of the person making the request and to locate the information which he seeks; or

(b) to the extent that he cannot comply with the request without disclosing information relating to another individual who can be identified from that information, unless he is satisfied that the other individual has consented to the disclosure of the information to the person making the request. The reference to information relating to another individual is restricted to a reference to information naming or otherwise explicitly identifying that individual as the source of information (paragraphs 14.37-39).

14.12 Whenever the data user withholds data on the basis of a statutory exemption, the data user should be legally required to inform the data subject of the exemption claimed unless doing so is likely to prejudice the purposes for which the data are kept or cause other serious harm. In such cases, data users should keep a log of cases in which a subject exemption is relied upon and the reasons for the exemption's use. The log should be available for inspection by the data protection authority and the authority should also be provided with a periodic return (paragraphs 14.46).

OECD Individual Participation Principle

14.13 This provides:

"An individual should have the right:-

(a) to obtain from the 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."

14.14 These access and correction rights are more tersely expressed in article 13 of the draft Directive.

Other jurisdictions

14.15 Data subject access and correction rights are a basic feature of the data protection laws of other jurisdictions. Flaherty points out[1] that access and correction rights are widely perceived in these jurisdictions as an incentive for record keepers to improve the quality of personal records. The rights create an awareness among data users that their activities are ultimately subject to public scrutiny. Inger Hansen, the former Canadian Privacy Commissioner, thought that when collectors of information are aware of an individual's right of access:

> *"the collectors act more responsibly and fairly. When the authors of reports know that their reports may not be kept confidential, language becomes cautious, derogatory assessments will be supported by examples when the examples only will be cited, leaving the reader to make up his or her own mind."*[2]

14.16 Statistics from other jurisdictions show that access rights are used by a significant proportion of the data subjects on whom they are conferred. In the UK, 100,000 requests, mainly addressed to large data users, were made in the few months after subject access rights came into effect[3]. They have since tapered off significantly.

---

1 David Flaherty, *op cit*, page 30.
2 Flaherty, *ibid*, page 271.
3 Home Office, *Review of the Data Protection Act: Report on Structure*, HMSO, 1990, page 3.

14.17 Subject access problems constitute a significant proportion of the complaints received by data protection authorities. Of the 1,747 complaints received by the UK Data Protection Registrar in 1991/2, 200 related to subject access.[4]

Our earlier recommendations

14.18 Before considering the mechanics of access detail, it may be useful to briefly reiterate several earlier recommendations of general relevance to the issue. It will be recalled that we propose the regulation of all personal data, regardless of whether it is in automated or non-automated form. Except as regards the application of the Security Safeguards Principle, this is subject to the limitation that the data must be reasonably practicably retrievable. Whilst all automated records will normally fulfil this requirement, it will be a question of fact whether non-automated records such as paper files do so at the time the request is received. This formulation is largely aimed at protecting data users from access requests which are unreasonably onerous to discharge, due to practical difficulties in locating the data sought. The formulation is not technology-bound and accommodates the fact that data which are not currently reasonably retrievable may become so. This may be due to administrative steps such as indexing, or technological ones such as feeding manual records onto a database with the assistance of optical scanners.

Individuals entitled to access

14.19 We recognise that personal data may be imported into Hong Kong from countries with inadequate controls. Upon its transfer here it will in effect be assumed to have been legitimately compiled in the absence of evidence to the contrary. The individual residing out of Hong Kong should be entitled to rebut this presumption by exercising his access and correction rights. **We therefore recommend that access and correction rights not be restricted to Hong Kong residents.**

The mechanics of subject access

14.20 The framing of a workable subject access provision requires consideration of a number of practical matters. These include such matters as the form of access requests, material to be provided, and fees. These matters are now discussed and recommendations made. Section 21 of the UK Data Protection Act provides a useful example for illustrative purposes. The discussion will refer to the practical operation of this provision as summarised in the annual reports of the Data Protection Registrar and further evaluated in the Home Office Review.

---

[4] Eighth Report of the Data Protection Registrar, June 1992, London: HMSO.

Material to be provided upon request

14.21 Under the UK provision an individual is entitled:

(a) to be informed by a data user whether the latter's data refer to that individual; and

(b) if so, to be supplied with a copy of that data. This is so even if the request is only for information regarding whether such data exist, as the provision states that such a request is to be treated as extending to being provided a copy if it does exist, in the absence of any indication to the contrary.

14.22 **We recommend the adoption of (a).** As to (b)'s treating an inquiry about data as a request for such data if they exist, we recognise that this approach will often be convenient for both the data subject and the data user. It obviates the need for a follow-up request for data once it has been confirmed that the individual is a data subject. In addition, ascertaining whether data are held on an individual will usually make it a simple matter to have the data copied, sparing the data user from the duplication of effort entailed in locating the relevant records twice. Neither the Registrar nor the Home Office mention any difficulties regarding the provision's operation. We can foresee difficulties, however, where thousands of pages of data are relevant and have not been specifically requested. We think it should be for the data user to assess the reasonableness of providing copies of data, failing an explicit request for such copies. **We recommend that, upon receipt of an inquiry as to whether data exists which is unaccompanied by a request for such data, the data user should have a discretion as to whether to provide a copy of that data, or to await a specific request.**

Provision of description of data purposes

14.23 The Home Office Review recommends (following the Registrar's 1989 review) that, in addition to confirming whether or not the applicant is a data subject and, if so, providing an intelligible copy of any such data, the data holder should supply the data subject with:

(i) details of sources and disclosure. The Review leaves open whether there should be an associated logging requirement. We rejected as overly onerous an across-the-board logging requirement in Chapter 10.

(ii) a statement of purposes for which data are held. The Review comments that this "is needed to complement the other information given in subject access so as to give the data subject some clue as to whether issues such as fair obtaining, adequacy or excessiveness arise in his case."

(iii) a statement that problems may be pursued through the Registrar.

The role of declarations

14.24 A perusal of data purposes as set out in an organisation's declaration will assist the data subject to narrow down the organisations meriting the exercise of a full access request. As some data subjects will discover what they need to know about an organisation's records system from a perusal of the declaration alone, thereby obviating the need to ascertain whether they are data subjects and to obtain a copy of data held, data users would be saved from having to provide a copy of any data held in response to every inquiry. We have recommended in Chapter 13 that public sector data users compile declarations which would include items (i) and (ii), but that private sector data users only need to address (ii). In both cases, the declaration's contents are relevant both to the individual's decision whether to make a request for a copy of all data relating to him and to provide a context to interpret the copy data subsequently supplied following such a request. The only additional issue requiring consideration is whether individuals should be provided with a copy of the declaration at either or both stages. It will be recalled that we envisage that in Hong Kong interested individuals would have ready access to on-line and print-out facilities to ascertain the contents of declarations. The question is whether, in addition, data users should be required upon request to furnish a copy of the declaration at the initial inquiry and/or the full access request stage. We consider this unnecessary in view of our other proposals. Nor do we think data subjects should be specifically told to pursue matters through the data protection authority, in case this deters them from initially following the matter up with the data user.

Fees

14.25 As mentioned above the UK Act treats all data subject inquiries as a request for a copy of any data relating to the inquirer. The Act imposes a separate access fee for each (automated) file entry. The 1989 review disclosed that the predominant view among data users was that a fee should be chargeable to discourage frivolous requests. Data subject representatives were concerned that the fee could discourage legitimate requests.

14.26 **We recommend that a nominal, waivable, fee be payable by a data subject merely inquiring as to whether data exist relating to him. To deter mischievous requests, a fee should be payable for full access requests which require the supply of a copy of data held. This objective should be fulfilled by a nominal fee, not one that is cost-related. The fee should accordingly be set at a moderate level. It should operate as a maximum, and organisations should be at liberty to reduce or even waive it.** In this regard we note that in the Federal Republic of Germany no charges are made for access to government files because of the difficulty and expense entailed in administering an accounting system.

14.27 This recommendation departs from the Consultative Document's proposal that there be no fee for merely making the inquiry. The amendment is to provide a potential minor deterrent to nuisance applications.

14.28 We also agree with Citibank's submission and have concluded that data users should not be restricted to nominal reimbursement when they had earlier provided that same data. **We therefore recommend as a proviso to the right to be provided a copy of data at a nominal fee that a fee may be charged on a commercial basis if a copy had been provided earlier. Alternatively, the data user may confirm if requested that the data provided earlier remains accurate.**

14.29 A general point made by some respondents is that, to the extent that fees are not cost-related, customers not exercising their rights would be subsidising those that do. The resultant correction of data benefits the data user, however, who may accordingly be disposed not to cost it. Citibank argued that there should be a cut-off date for corrections. We take the view that it would be unreasonable to impose such a restriction.

14.30 Where the data user has separate entries in his declaration concerning different purposes, the issue arises whether the data subject should be charged a separate fee for a copy of the data for each purpose. The UK Act does charge for each entry, but the general view is that a maximum fee level should be set.

Should the data protection authority set fees?

14.31 On the general question of the level of fees, we recognise that the data protection authority is not a disinterested party on this issue. It may accordingly be preferable for levels to be set elsewhere. Once determined, the inclusion of fees in subsidiary legislation would facilitate updating as required. **We recommend that the question of fees be provided for in subsidiary legislation.**

Form of request

14.32 We have considered the form in which an individual should request an organisation to confirm whether it holds data on him and, if so, to provide a copy of that data. Administrative difficulties may arise if requests requiring the payment of fees are unrecorded. The onus of providing that record should be on the individual making the request. **We recommend a requirement that requests be in a recorded form, although data users may waive this requirement and accept requests by terminals or telephone.**

Intelligibility

14.33 **We recommend the adoption of a general requirement that data provided in response to access requests be in an intelligible form, unless it is a true copy of a written document which is unintelligible on its face. Data should be supplied in the language in which it is held and, where data is held in more than one language, it should be provided in both languages.** In most cases, the languages concerned are likely to be Chinese and English but we have deliberately worded our recommendation to cover the situation where, for instance, a Japanese bank held data in Japanese and English.

14.34 This recommendation replaces the Consultative Document's proposal that "data users should respond in the language of the access request when this is in Chinese or English. When this entails a translation, it should be provided by the Privacy Commissioner at a nominal fee". On reflection, and in the light of submissions received, we consider that this would place an unreasonable burden on the limited resources of the Privacy Commissioner. We would hope that the larger commercial organisations would voluntarily provide data in both Chinese and English but we do not think it right for us to seek to impose a statutory requirement to this effect across the board.

14.35 The Hong Kong Medical Association submitted that the intelligibility requirement posed problems in providing access to a doctor's notes. We take the point that such notes are largely an account of the doctor’s thought processes, including his speculations regarding diagnosis. Their intelligibility will often be an issue. Nonetheless, we think that our present general recommendation of an intelligible copy should not be departed from with doctors notes. Our proposed exemptions regarding access where harm could result to the patient should protect against harmful disclosures.

Time limits

14.36 In the Consultative Document we proposed that access requests be responded to within 30 days. Several respondents, including American Express Bank, sought a 60 day period. Their concern was that locating old records could be time consuming and legal advice may be required on whether an access exemption applied. On the other hand, granting too long a period could generate extra inquiries from worried individuals for the Privacy Commissioner to chase up. **We therefore recommend that access requests be complied with within 45 days. We note that the UK law specifies 40 days. We have also substituted "comply" for "respond to" because the latter would arguably be satisfied by merely acknowledging the request.**

Limitations on data access

14.37 Section 21(4) of the UK Act provides that a data user is not obliged to respond to subject access requests:

> *"(a) unless he is supplied with such information as he may reasonably require in order to satisfy himself as to the identity of the person making the request and to locate the information which he seeks.*
>
> *(b) if he cannot comply with the request without disclosing information relating to another individual who can be identified from that information, unless he is satisfied that the other individual has consented to the disclosure of the information to the person making the request."*

14.38 The Registrar reports receiving strong representations that without data subject assistance in locating data, answering requests would be "simply not practicable." The second requirement, that of reasonably satisfying the data user of the applicant's identity, is also an important one. It is necessary to protect the privacy of other data subjects. But we consider the UK formulation too broad. The provision does not make clear that data users should comply with requests insofar as it is possible to do so without disclosing the identity of the other person referred to. Often this will be readily achievable by editing out names. Where the problem is not resolvable in this manner, it should be the responsibility of the data user to seek the consent of the other person that his identity be disclosed. **We recommend that both these requirements be adopted in Hong Kong, but that (b)'s commencing words "if he" be replaced by "to the extent that he".**

14.39 We agree with the general aim of section 21(4)(b). Its operation is elaborated on by section 21(5). That provides that the reference to information relating to another individual includes a reference to information identifying that individual as the source of information. **We similarly recommend that there be no obligation to respond to the extent that the data names or otherwise explicitly identifies an individual as the source of information.** This qualification of access rights is necessarily narrow and will only entail editing out the identification. It would not defeat access where explicit identification is lacking but the source can be readily inferred. Refusing access to data to the extent that it inferentially identifies a source will require the sanction of one of the public interest exemptions detailed in Chapter 15.

"Forced access"

14.40 In his 1989 review of the UK Act, the Data Protection Registrar recommended that it be made a criminal offence to require the data subject to exercise his subject access rights to reveal his criminal record. Article 13(2) of the draft Directive is both broader and weaker. It provides that a data

subject shall have the right to refuse any third party demand to exercise his access rights, unless required to do so by law. While we prefer the latter approach, we view it as a data collection issue. If the data are insufficiently relevant, the requirement would contravene the collection principles discussed in Chapter 9. If the data are relevant, we think it should be a matter for the data subject whether he accedes to the request, unless it is thought appropriate to prohibit it in the legislation dealing with specific sectors such as employment. To this extent we agree with the draft Directive provision, but do not consider that the issue need be specifically adverted to in the data protection legislation.

14.41 Several submissions have criticised the fact that we declined to provide the data subject with specific protection against third party demands that he exercise his access rights. The UK Data Protection Registrar's submission generally refrains from policy advice, but on this issue he provides the following warning:

> *"Enforced subject access has been a particular issue in the UK, as stated in the 1989 Annual Report. The Registrar is aware of many cases where, in order to obtain employment, a data subject has been required by a prospective employer to exercise his subject access rights to obtain a copy of his police record. This practice has been particularly prevalent in licensing by local authorities and in the private security industry. We are also aware of cases of enforced subject access in connection with insurance claims where, for example, an insurance company may believe that the claimant has not given full information about past claims history. While the revised draft Directive is helpful in giving the data subject the right to refuse to exercise his subject access rights in this way, in practice his room for manoeuvre may be limited by his need for the job, or for settlement of the claim. The Registrar's view is that subject access rights exist to enable an individual to know what is held on computer about him, not to enable others to have this information."*

14.42 Similar concerns are expressed by the Bar Association. We think it is important to remember that the right of access is a right accruing to the data subject, not the data user. Access at the behest of a data user runs counter to this. However, to introduce a criminal sanction in all cases against a data user requiring the individual to exercise his access rights would run the risk of criminalising what in some cases many would consider reasonable conduct. We have concluded that we should not take steps at this stage to prohibit requests to the data subject to obtain access on behalf of the data user. If experience shows a substantial level of abuse, then this is an area which may need to be examined anew.

Exemptions to data access

14.43 The preceding section dealt with general limitations on subject access, irrespective of the subject matter or purposes of the data. But data protection interests are not absolute. Social realities require that the exercise of such rights must on occasion be restricted by competing considerations. Accordingly, in the following chapter, we make detailed recommendations regarding data purposes which should be exempted from the general requirements of a data protection law, including access requirements. We recommend that the data protection law, including access requirements, should have no application to personal data held by an individual solely for private and personal purposes. This includes personal correspondence. We further recommend that the data protection law should apply to data held for such purposes as law enforcement, but that agencies holding such data should be exempted from the requirement that they must provide direct access where the record keeping purpose is likely to be compromised. Similarly, we recommend an exemption from data access requirements where serious harm is likely to the physical or mental health of the data subject, such as with sensitive medical and social work data.

Giving reasons for claiming access exemptions

14.44 Whilst determining appropriate subject access exemptions is a complex issue requiring a detailed treatment better reserved for a separate chapter, a related issue of a general nature may be dealt with at this stage. The UK Registrar reports in his 1989 review of a difficulty that had arisen when information is withheld under a subject access exemption but the individual is not given details. The UK law does not require data users to identify the nature of the exemption claimed, nor does the Registrar recommend such a requirement as:

> *"the statute plainly sees circumstances in which granting subject access would prejudice the purpose for which data are kept, or cause other serious harm. It seems highly likely that there will be cases where to tell a data subject that data have been withheld for these reasons would cause the same damage contemplated by the statute."*[5]

14.45 While we take the Registrar's point, we also share his concern that denying the data subject details of exemptions claimed could prejudice his exercise of review or appeal rights. The Registrar's recommended remedy is to require data users to keep a log of cases in which a subject exemption is relied upon and the reasons for its use. The log is to be available for inspection by the Registrar and he is also to be provided a periodic return.

14.46 The Registrar's recommendation would appear to provide a useful check on the claiming of exemptions, but we are not sure if his

---

5 Fifth Report of the Data Protection Registrar, June 1999, London: HMSO.

recommendation goes far enough. We accept that the distinction between the reason for withholding the data and its content is not always a neat one. Nonetheless, it is not evident that identifying the exemption will always cause the same damage as disclosing the data. **We therefore recommend that upon withholding data, the data user be legally required to inform the data subject of the exemption claimed unless doing so is likely to prejudice the purposes for which the data are kept or cause other serious harm. Regarding these cases, we recommend the adoption of the Registrar's logging proposal.**

Transition period

14.47 In Chapter 8 we recommend that access rights accrue immediately upon enactment of the law, but in a qualified manner during a transitional period.

Chapter 15

Exemptions

Summary

15.1 Data protection laws seldom attempt to regulate all data uses. Two alternative approaches are possible:

(i) a law of general application but with specific exemptions; or

(ii) a law restricted to specified data users.

15.2 We propose adopting the first of these alternatives. This is the approach generally adopted in other jurisdictions and makes it easier to amend the law as circumstances change.

15.3 Exemptions may be provided because:

(i) the record keeping activities concerned may have little impact on privacy interests, such as data held by an individual solely for his personal purposes;

(ii) the social importance of the exempted data purposes is thought to outweigh the privacy interests; or

(iii) there are public interest reasons for exempting the data from subject access.

15.4 Exemptions may be from all or some of the requirements of the data protection law. Total exemption frees a data use from the application of all the data protection principles and all administrative requirements. The only total exemption we recommend is for data held by an individual solely for private purposes.

15.5 Partial exemption frees a data use from compliance with one or more of the principles or administrative requirements. In reaching our conclusions we have borne in mind the OECD's stricture that exemptions should be "as few as possible, and they should be made known to the public."[1]

15.6 The discussion in this chapter is concerned with the exemptions to be included in the principal data protection legislation. Other ordinances

[1] OECD Guidelines, *op cit*, paragraph 46.

will also effect partial exemptions and Chapter 3 examined the legislation that may partially overlap the operation of a data protection ordinance.

Recommendations

15.7 There should be a total exemption from the requirements of a data protection law for personal data held by an individual and concerned solely with the management of his personal, family or household affairs or held by him solely for recreational purposes (paragraph 15.22).

15.8 No exemption from the application of the data protection law should be made for non-profit making bodies (paragraph 15.23).

15.9 The Use Limitation Principle should not apply:

(i) to data required by or under any enactment to be made available to the public (paragraph 15.25)

(ii) where it would be likely to prejudice the prevention of serious injury or other damage to the health of any person, the prevention or detection of crime, the apprehension, prosecution or detention of offenders, or the assessment or collection of any tax or duty; (paragraph 15.38)

(iii) where the disclosure relates to conduct that is illegal or seriously improper and the person making the disclosure had reasonable grounds for believing that the disclosure to the person receiving it would contribute to the prevention or remedying of the unlawful or seriously improper conduct (paragraphs 15.45 and 47); or

(iv) where the disclosure relates to the character or activities of an individual where this is likely to seriously affect the performance of the functions of a statutory body or administrative tribunal (paragraph 15.48).

15.10 The Privacy Commissioner may exempt research data that has not been irreversibly anonymised from the application of the Purpose Specification and Use Limitation Principles. In providing his consent the Privacy Commissioner would need to be satisfied that the research is in the public interest, having regard to the following safeguards:

(i) whether access to data identifying individuals is necessary for the scientific validity of the research;

(ii) whether access to that data without the data subject's consent is justifiable in the circumstances;

(iii) whether the researcher has undertaken to comply with the relevant code of conduct; and

(iv) whether the research results are to be anonymised, except to the extent that this is outweighed by the public interest (paragraph 15.50).

15.11 There should be an exemption from access and correction rights:

(i) to the extent that the release of the data would be likely to prejudice the prevention or detection of crime, the apprehension, prosecution or detention of offenders, the assessment or collection of any tax or duty, regulation of financial institutions, markets and industry, or identify any individual disclosing data within the scope of the exemption from the Use Limitation Principle specified in paras. (iii) and (iv) of paragraph 15.9 (paragraph 15.52);

(ii) to data received from third parties relevant to the making of judicial appointments (paragraph 15.54);

(iii) to data to which a claim for legal professional privilege can be made out (paragraph 15.55);

(iv) to data the release of which is likely to cause serious harm to the physical or mental health of the data subject (paragraph 15.57);

(v) to staff succession planning data (paragraph 15.64);

(vi) interim access to data relating to an evaluative process which will be seriously disrupted by affording access before a decision has been made and where appeal rights exist. The data must be retained following the making of the decision, when access rights accrue (paragraph 15.65); and

(vii) personal references supplied on a confidential basis by a person not under a duty to supply these to the organisation seeking to fill a vacancy. The exemption should cease to apply upon the position being filled (paragraph 15.77).

15.12 For the avoidance of doubt, the statutory definition of "personal data" to which the access provisions apply should expressly exclude criteria of general application. Insofar as a decision may be expressed cryptically, the requirement that the data be provided in an intelligible form does not entail the decoding of the applicable criteria (paragraph 15.62).

15.13 Except in the case of data held for the purposes of the security, defence or international relations in respect of Hong Kong, the Privacy Commissioner shall upon application review the release of data where the

data user has claimed an access exemption. The initial responsibility in fully responding to access requests lies with the data user. The statutory language should make it clear that access requests should be complied with insofar as it is possible to do so without prejudicing the exempted purpose (paragraph 15.80).

15.14 Data held for the purpose of the security, defence or international relations in respect of Hong Kong should be exempted from access and correction rights and from the application of the Use Limitation Principle whenever that interest is likely to be otherwise prejudiced. A certificate personally signed by the Governor or Chief Secretary would be evidence of the exemption. This power should not be delegable. Data users would nonetheless remain subject to the general requirement of furnishing declarations describing in general terms the data held for these purposes. In addition, the other data protection principles would apply. As regards the data identified in the certificate, he would be entitled to look behind the certificate of the Governor or Chief Secretary to confirm that the data purpose for which the exemption was claimed was correctly classified as relating to the security, defence or international relations in respect of Hong Kong (paragraph 15.87).

15.15 Upon receiving a complaint concerning data relating to the security, defence or international relations in respect of Hong Kong, the Privacy Commissioner should be entitled to monitor compliance with the data protection principles. The Privacy Commissioner will only indicate to the data subject that he has made all necessary inquiries and will not disclose whether there is a file on the inquirer. This will preclude the complainant from pursuing any appeal to the tribunal (paragraph 15.91).

15.16 The Council of Europe recommendations regulating the use of personal data in the police sector should be used as the basis for deriving a similar code suitable for Hong Kong (paragraph 15.92).

Data purposes with limited privacy implications

Data used solely for private and personal purposes

15.17 Article 2 of the draft Directive provides that it shall not apply to "the processing of personal data by a natural person in the course of a purely private and personal activity." The basis of this total exemption is that invasions of privacy are thought unlikely to occur. This draft Directive exemption is included in many domestic laws. The United Kingdom Act, for example, exempts:

> *"personal data held by an individual and concerned only with the management of his personal, family or household affairs or held by him only for recreational purposes."*

15.18 It will be observed that both provisions advert to two related requirements. The first is that the entity to be exempted is an individual and

not an organisation. Secondly, the data must be held solely for private and personal purposes. The two requirements are linked because, quite apart from the semantic point that an organisation cannot have "personal" purposes, organisations are more subject than individuals to operational imperatives which affect data subjects. Organisations obtain data as a basis for making administrative or commercial decisions affecting the data subject. They are also likely to participate in the exchange of personal data.

15.19 Data held by an individual solely for his personal purposes may be compiled by himself (eg a Christmas card list) or provided by another (eg a personal letter). The exemption only applies for as long as the purpose is not altered. If the individual discloses a copy of the list or letter to a government department or company, the exemption would cease to apply.

Earlier recommendations

15.20 One of our earlier recommendations distinguished between individuals and private sector organisations. Although the data protection principles would apply to both (unless exempted), only the latter would be required to furnish declarations. The draft Directive goes further and exempts an individual from the principles as well, but only if held solely for private and personal purposes.

Justifications for exempting data solely for personal use

15.21 There are several justifications for the exemption:

(i) There is comparatively little potential for the data protection principles being infringed to the detriment of data subjects when data are held solely for personal purposes. An example would be a private address book. The very terms of the exemption preclude an individual from transferring data for purposes not initially envisaged. Even if data quality is poor, if kept solely for his personal purposes it will only influence the individual's perception of the data subject. Of course, if he fails to reasonably safeguard the material, it could find a wider audience. Whilst ideally an individual should maintain accurate and securely stored personal data about others, it would be unduly onerous to impose a legal requirement to this effect.

(ii) Subjecting such material to the principles and in particular to subject access rights may constitute a violation of the privacy of the data user and others. This would appear to follow from the terms of article 14 of the BOR. This is set out in Chapter 2 and provides the right to legal protection against "arbitrary or unlawful interference" with a person's correspondence.

A concrete example may assist. A writes a personal letter to B containing opinions about C. B files it away in an indexed manila folder solely for his own personal use. C wishes to see any letters which B has referring to him. To grant him access would interfere with both A and B's privacy of correspondence. Often data received by another and held solely for private purposes will have been provided in confidence. The issue of confidentiality is independent of the operation of the BOR and is dealt with below.

The position would be different in the above example if B acted on the opinions in making hiring/firing decisions on behalf of his organisation. This would demonstrate that it was no longer being held solely for personal or domestic purposes, as he would be applying it for the purposes of his organisation. Accordingly, personal data fall outside the ambit of this exemption if the data are either:

(i) entered as a non-personal record, such as on a company data base, or

(ii) used for a non-personal purpose, such as the basis of a decision regarding company operations.

Recommendation

15.22 **We recommend that there be a total exemption from the requirements of a data protection law for personal data held by an individual and concerned solely with the management of his personal, family or household affairs or held by him solely for recreational purposes.**

Non-profit making bodies

15.23 The revised draft Directive has abandoned its earlier complete exemption for records held by non-profit making bodies, provided they relate solely to members and are not communicated to third parties. Under the revised proposal they are only to be exempted from the administrative requirement of furnishing the supervisory authority with a declaration. The Consultative Document proposed to follow a similar course. On further reflection, we think that such an approach introduces a needless complication to the scheme we propose, not least because of the difficulty of identifying non-profit making bodies. In addition, the exemption from a requirement to *lodge* a declaration is meaningless: the non-profit making body would nevertheless be obliged to *prepare* a declaration. **We accordingly recommend that no exemption from the application of the data protection law should be made for non-profit making bodies.**

Other data purposes arguably not infringing privacy

15.24 The United Kingdom Data Protection Act completely exempts personal data held solely for pensions, payrolls and accounts. The Registrar has commented[2] that these exemptions have caused considerable confusion among data users and that if data users are only required to comply with simple administrative obligations under the legislation, it may be appropriate to remove these exemptions altogether. We agree that it is desirable to avoid the creation of a confusing patchwork of exemptions. We see no reason in principle why this data should not be subject to the data protection principles.

Public records

15.25 Some data protection laws completely exempt public registers. Yet certain registers, although ostensibly "public", clearly envisage specific data purposes. A local example is provided by electoral records. This is compiled for electoral purposes, pursuant to a statutory duty to furnish the requisite data, some of which is sensitive. The data is publicly available solely to facilitate public scrutiny of the data to secure fulfilment of the statutory purpose. An exemption would sanction data collected for such purposes being used for another purpose not originally envisaged by the person furnishing the data. The difficulty that we have had to face, however, is that the public availability of such data renders unenforceable a prohibition of its use for different purposes. We have reluctantly concluded, therefore, that it is impractical to attempt to constrain the data purposes of publicly available data. Although the revised Directive does not so provide, we note that a number of countries partially exempt publicly available data, including the UK, Belgium, Ireland, Luxembourg and the Netherlands. In all these cases, however, the exemption only applies to data which are required by law to be made public. We think that this must be right. If the test were simply whether the data were in the public domain, it would provide data users with the opportunity to subvert the law by publicizing the data. **We therefore recommend that there should be an exemption from the application of the Use Limitation Principle for data which are required by or under any enactment to be made available to the public, whether by publishing the data, making the data available for inspection or otherwise, and whether gratuitously or on payment of a fee.** Should the data be applied for another purpose, the data protection law would apply at that point. For example, upon electoral data being applied for direct marketing purposes, it would become subject to the application of the principle. **We also recommend that the other principles apply, including those dealing with the correction of data and compensation for inaccurate data.** It is for public authorities to consider whether specific restrictions on the use of such data should be included in the relevant legislation. Without restrictions people may become less candid in furnishing data in order to avoid the data's subsequent dissemination.

---

[2] Fifth Report of the Data Protection Registrar, June 1985, London: HMSO, 1985.

Public interest exemptions

15.26 Data protection interests are not absolute. Social realities require that such rights must on occasion be limited by competing public interests. Human rights jurisprudence has established, however, that these limitations should be necessary for the exercise of the competing interest. This issue is discussed below.

Identifying social interests requiring exemptions

15.27 Various public interests have been identified in data protection laws as meriting exemption from some or all of the principles, such as national security and public safety. Exemptions for these purposes may be at several levels, namely total exemptions, or only from one or more of the data protection principles. This is reflected in the United Kingdom Act. Data held for national security purposes are granted the broadest exemption. Data held for the control of crime and collection of taxation are exempted from the principles limiting disclosure (the OECD equivalent is the Use Limitation Principle) and providing access rights. The exemption only applies on a case by case basis where the application of either or both of these principles is "likely to prejudice" these competing interests. A number of data purposes are exempted only from subject access rights, namely health and social work, the regulation of financial services, judicial appointments and legal professional privilege. An exemption from the non-disclosure principle only is accorded data where the disclosure is urgently required for preventing injury to health. Except for national security, data exempted from access/correction rights and/or the principle limiting disclosure are subject to all the other principles, and to registration requirements precluding secret databases.

15.28 Whilst we broadly agree with the structure of the United Kingdom Act's treatment of exemptions, we consider some of the provisions overly restrictive of access rights. A relevant factor is that we have to take into account the Bill of Rights. The relevance of this legislation (which has no United Kingdom equivalent) will now be briefly reviewed.

Exemptions and the Bill of Rights

15.29 We saw in Chapter 2 that information privacy is a protected right under the BOR. Whilst article 14 does not explicitly advert to data protection, the matter is addressed in the Human Rights Committee's general comment on the corresponding provision in the ICCPR. The full comment is set out in Chapter 2. The last chapter highlighted the data subject's right to:

(i) ascertain which public or private bodies control his files;

(ii) ascertain what data are so held; and

(iii) request rectification or elimination of incorrect personal data.

15.30 These rights are recognised in the Human Rights Committee's general comment, at least as regards automated data. The Hong Kong Court of Appeal held in *R v. Sin Yau Ming*[3] that such comments will be accorded considerable weight in determining the scope of the identically worded provision in the BOR. It is accordingly strongly arguable that access and correction rights are protected under the BOR and access exemptions constitute *a prima facie* violation of these rights requiring justification. *Leander v. Sweden*[4] is a persuasive authority on the appropriate approach to the question. It will be recalled in that case (discussed in Chapter 2) the European Court of Human Rights considered the corresponding provision of the European Convention for the Protection of Human Rights and Fundamental Freedoms. The court held that the storing and disclosure of the highly sensitive data there involved, coupled with a refusal to allow Mr Leander an opportunity to refute it, amounted to an interference with his right to respect for his private life. The main issue was whether this restriction on the applicant's access rights was justifiable. The court accepted that it was necessary for Sweden to have a system for controlling security-sensitive posts, provided that the system contained adequate and effective guarantees against abuse. In the absence of access rights, the court had to examine the adequacy of other controls. These controls consisted of the presence of parliamentarians on the body releasing the data. Further supervision was provided by other independent oversight agencies, such as that of the Ombudsman. The court held that these controls provided adequate protection against abuse. The essential point in the present context is that the onus was on the party denying access to show that adequate alternative controls existed. *Leander* is persuasive authority for the proposition that denial of access rights to information relating to one's private life coupled with a lack of alternative controls on the use of such information may infringe article 14 of the BOR.

The submissions

15.31 The BOR only applies to the public sector. Of the submissions received, only two submissions (those of the Registrar General and Far East Trade Press Ltd.) expressly questioned the need for data protection regulation. One submission from the financial sector originally sought a general exemption from the data protection law for the private sector but subsequently conceded that that sector would be subject to some form of legislative restriction. Indeed, we believe that the international trade argument for regulation developed in Chapter 2 is particularly relevant to the financial sector.

15.32 Against this background we now examine data purposes involving dominant social interests meriting exemptions from a data protection law. The discussion distinguishes exemptions from the Use Limitation

[3] [1992] 1 HKCLR 127.
[4] (1987) 9 EHRR 433.

Principle from exemptions from access and correction rights, as the two exemptions raise different considerations. It will be seen, however, that a number of public interests arguably merit exemption from both.

Exemptions from the Use Limitation Principle

Exemptions proposed in the Consultative Document

15.33 It will be recalled that the Use Limitation Principle requires that data "should not be disclosed, made available or otherwise used for purposes other than those [originally specified]." The principle would apply to both the person passing on the data and to the person receiving the data in contravention of the original purpose(s). In the Consultative Document we proposed that the principle not apply to data in respect of the security of Hong Kong and where compliance would prejudice the following competing public interests.

15.34 **Public health and safety** Section 34 (8) of the United Kingdom Data Protection Act exempts from their equivalent of the Use Limitation Principle personal data "in which the disclosure is urgently required for preventing injury or other damage to the health of any person or persons." We recommend the adoption of this exemption in Hong Kong, subject to its being limited to "serious" injury.

15.35 **Prevention of crime** We had endorsed the United Kingdom Act's formulation of "the prevention or detection of crime or the apprehension or prosecution of offenders". In the light of a submission from the Correctional Services Department that this exemption may not sufficiently cover data relating to the detention of prisoners; we recommend that it should extend to the apprehension, prosecution *or detention* of offenders. The Royal Hong Kong Police were concerned that "crime" might not be wide enough to include all offences. We do not foresee difficulties in this regard, and note that the UK Data Protection Registrar has not encountered any problem.

15.36 A number of submissions were made to us by bodies involved in the prevention, investigation or prosecution of crime, arguing that specific exemptions should be made for their functions. We have carefully considered these submissions in the process of formulating our proposed general exemptions from both the Use Limitation Principle and access and correction rights.

15.37 **Taxation** The Consultative Document endorsed the United Kingdom Act's reference to "the assessment or collection of any tax or duty". We note that in his submission the Commissioner of Inland Revenue endorses an exemption in these terms, together with the exemption discussed below regarding access to data which is likely to prejudice these statutory purposes.

15.38 **To sum up, we recommend that the Use Limitation Principle not apply where it would be likely to prejudice the prevention of serious injury or other damage to the health of any person, the prevention or detection of crime, the apprehension, prosecution or detention of offenders, or the assessment or collection of any tax or duty.** This is a matter to be determined on a case by case basis depending on the purpose of the specific data in question. It cannot be assumed that all personal data held by the police, for example, will fall within the terms of the exemption. Personnel records would not, for example.

Additional exemptions proposed by respondents

15.39 In addition to the submissions adverted to above, we have received submissions from regulatory bodies specifically seeking an exemption from the Use Limitation Principle to secure the flow of information about individuals whose activities could adversely affect their statutory functions. The Hong Kong Monetary Authority ("HKMA") monitors authorised institutions and comments:

> *"Part of the information necessary to the evaluation of proposed office holders of authorised institutions is obtained through inquiries about the data subject with the police, ICAC, Official Receiver's Office, other government departments and other regulators, including perhaps those abroad. Ad hoc enquiries may also be made with other persons who may have information about the data subject, e.g. former employers, colleagues, business contacts etc. The enquiries described will generally be made without the knowledge or consent of the data subject. The objective is to build up a full picture of the individual concerned so that the HKMA may satisfy itself that the individual is fit and proper for a position with an authorised institution."*

15.40 The HKMA adds that even where an individual is not applying for, or occupying, such a position, it may still be relevant to the statutory functions of the HKMA to gather information about that individual, such as where an individual has significant business dealings with an authorised institution. This highlights the overly restrictive exemptions proposed in the Consultative Document, for these focused on the appointment of office holders.

15.41 Other bodies in a similar situation to the HKMA can be readily identified and would include:

(i) the Independent Commission Against Corruption, in its monitoring of the "cleanliness" of government;

(ii) the Commissioner of Insurance, as he must ascertain the fitness and propriety of directors and controllers of insurance companies, with a view to protecting policy holders;

(iii) Urban Services, in determining the suitability of licence and permit holders;

(iv) the Transport Department in considering licensing applications;

(v) the Securities and Futures Commission, in regulating those in the industry; and

(vi) the Trade and Industry Branch in the course of appointing non-officials to government advisory boards and committees as well in making nominations for receiving honours.

15.42 We have concluded that a general exemption should be granted from the Use Limitation Principle to accommodate the activities of these bodies and their sources of information. The exemption would sanction the use of data for a purpose contrary to that for which it was acquired to assist them in fulfilling their functions. Such an exemption would have to apply both to the person providing the information for the public good and to the agency receiving it. Such an exemption is necessary even assuming that the data protection law will not abrogate existing statutory powers. This is because the legislation constituting these agencies does not necessarily sanction all their data gathering activities. For example, the Banking Ordinance provides that the HKMA may require a narrow class of "specified persons" to furnish information, and not the wide range of individuals their submission refers to. (The Ordinance also authorises the HKMA to pass on such information to other regulators).

15.43 The more difficult question is the proper scope of an exemption from the Use Limitation Principle to accommodate the competing social interests involved. While the Consultative Document identified law enforcement and taxation as two such items, the submissions establish the need for an exemption of sufficient generality to cover disparate situations, but no broader than is strictly required to address real social mischief.

15.44 In considering this issue, we have derived assistance from the public interest tests developed in the context of a defence to media intrusions into privacy. This issue was recently addressed by the Calcutt Committee.[5] They concluded that it should be a defence that the defendant had reasonable grounds for believing that his actions would protect one of the public interests identified above (crime, public health or safety) or expose "seriously anti-social conduct". In his subsequent Review,[6] Sir David Calcutt gives an example of the sort of conduct this expression would encompass, namely the business practices of Peter Rachman:

> *"Rachman had developed a technique of buying run-down property cheaply, because it was partly occupied by statutory tenants, who were hard to remove legally. He filled the flats with*

[5] Home Office, Report of the Committee on Privacy and Related Matters, HMSO 1990.

[6] Department of National Heritage, Review of Press Self-Regulation, HMSO 1993.

people whom he expected would enjoy noisy parties. This provoked the tenants into moving elsewhere. Rachman then got rid of the new tenants and was left with empty properties that he could sell at a large profit. That type of behaviour provides a striking example of 'seriously anti-social conduct'." (paragraph 7.21)

15.45 Notwithstanding that there would be clear cases, Sir David Calcutt conceded that "it might be considered too difficult a concept" for incorporation into criminal rather than civil legislation. We also find it somewhat vague and instead **we recommend that the general test be that the disclosure relate to conduct that is "illegal or seriously improper".** This formulation should encompass a breach of regulatory codes of conduct such as, for instance, those enforced by the Securities and Futures Commission. It would also cover breaches of professional codes. (This is on the assumption that such codes are in the general public interest and we recognise the possibility that a professional cartel may impose a regime which is unduly protectionist). But whilst we think that "illegal or seriously improper" would include contravention of codes, the ambit of these words would not be confined to this. Practices that are contrary to the public interest will precede codes, the formulation of which will be in response to these precipitating problems.

15.46 In addition to pertaining to the public interest, we think that the exemption should only extend to those disclosures which may reasonably further the public interest. We agree with the Calcutt Committee's requirement that the person making the disclosure must:

(i) have reasonable grounds for believing, (i.e. an objective test) that

(ii) the disclosure will contribute to, or is necessary for, the furtherance of the interest in question.

15.47 In the context of a defence to publication by the media, this nexus test is sufficiently precise, but as a general exemption from the Use Limitation Principle elaboration is required. This is to exclude the exemption's application from sanctioning busy-body disclosures made to those who cannot be expected to remedy the problem. The disclosure must be to a person with a specific interest in the matter. This may mean disclosure to the relevant public authority. Not all public interests are dealt with institutionally, however, and we therefore think that the essential test should be whether the recipient is the organisation or individual whose duty it is to consider the matter and take the necessary action. **We accordingly recommend the exemption should only apply where the person making the disclosure had reasonable grounds for believing that the disclosure to the particular individual involved would contribute to the prevention or remedying of the unlawful or seriously improper conduct in question.**

Extension for statutory bodies

15.48 This new recommendation exempting from the Use Limitation Principle disclosures about illegal or seriously improper conduct will provide some protection to "whistleblowers". It should also largely address many of the operational requirements of respondents. A vital function of regulatory agencies is the monitoring of key appointments. The supervision of the financial markets, for instance, entails ensuring that only fit and proper people are allowed to run businesses entrusted with the public's savings and investments. The candid exchange of personal information is vital in determining the fitness of office holders of such businesses. It is clear from submissions we received, however, that to apply the exemption only in respect of office holders would be too restrictive, as was pointed out by HKMA:

> *"Even where an individual is not applying for, or occupying, such a position, it may still be relevant to the statutory functions of the HKMA to gather information about that individual. This would be the case, for example, where an individual had significant business dealings with an authorised institution or, in extreme cases, was suspected of committing a fraud against it. This latter point illustrates that the activities of the banking supervisor can at time be akin to the law enforcement authorities, i.e. involving the collection of various types of intelligence, including information about individuals, which in some cases at least is relevant to the prevention or detection of crime."*

For that reason, we believe that it is necessary to widen the scope of matters that may be divulged. **We accordingly recommend an exemption from the Use Limitation Principle where the disclosure relates to the character or activities of an individual and this is likely to seriously affect the performance of the functions of a statutory body or administrative tribunal.** The principle should extend to administrative tribunals to enable, for example, professional tribunals to be apprised of the incompetence of their members.

Research data

15.49 A strict application of the Purpose Specification and Use Limitation Principles would prohibit the anonymisation of data then used for research, as it would constitute a new data purpose. Several submissions pointed out that the Consultative Document omits any exemption for survey or research data. The Chinese Manufacturers Association fears that the lack of an exemption for non-profit making organisations will adversely affect the target size of organisations used in surveys, and hence the validity of surveys. The Hong Kong Medical Association notes that research may entail the use of patient data that was not foreseeable at the time, such as a retrospective study of a group of patients with a specific disease. The Hong Kong Computer Society points out that research conducted by tertiary institutions is already covered by the relevant ethical codes of conduct in force at all

University and Polytechnic Grants Committee institutions. Statistical or research purposes constitute a data purpose to be specified like any other. Upon data being irreversibly anonymised it will no longer constitute "personal data" and will not be subject to the data protection principles. However, statistical data may remain data subject identifiable, or it may be anonymised, but subject to possible re-identification through the combination of variables.

15.50 **We recommend that the Privacy Commissioner be empowered to exempt research data that has not been irreversibly anonymised from the application of the Purpose Specification and Use Limitation Principles. In providing his consent the Privacy Commissioner would need to be satisfied that the research is in the public interest, having regard to the following safeguards:**

(i) whether access to data identifying individuals is necessary for the scientific validity of the research;

(ii) whether access to that data without the data subject's consent is justifiable in the circumstances;

(iii) whether the researcher has undertaken to comply with the relevant code of conduct; and

(iv) whether the research results are to be anonymised, except to the extent that this is outweighed by the public interest.

Exemptions from Access and Correction Rights

The submissions

15.51 The OECD refers to access and correction rights as "fundamental" and "perhaps the most important privacy protection". The submissions received generally accepted the principle espoused in the Consultative Document that the individual should have the right to access and correct factual data held about him. Where reservations were expressed they mainly related to the resource implications of handling a large number of requests. We also received a number of submissions opposing, in varying degrees, data subject access and correction rights to evaluative data. Some submissions also opposed access to data obtained in confidence. Some submissions merged these two issues, but they are analytically distinct and the discussion below distinguishes them.

General access exemptions

15.52 Before addressing any additional qualifications of access rights required by certain evaluative data, we now set out the general scheme of public interest exemptions from access and correction rights to data, whether it is factual or evaluative. These generally coincide with the exemptions

discussed above dealing with the Use Limitation Principle. **We recommend an exemption from the right of the individual to access and correct data relating to him:**

(i) where the release of the data would be likely to prejudice the following:

(a) the prevention or detection of crime or the apprehension, prosecution or detention of offenders;

(b) the assessment or collection of any tax or duty;

(c) the regulation of financial institutions, markets and industry;

(ii) to the extent that it would identify any individual disclosing data pertaining to (i), or disclosing illegal or seriously improper conduct or the character or activities of an individual where this is likely to seriously affect the performance of the functions of a statutory body or administrative tribunal.

15.53 We wish to emphasise that although these are similar to the public interest categories we identified for exemption from the Use Limitation Principle, it does not follow from the limited sanctioning of passing on of data for a different purpose that access should be denied. Rather, it strengthens the need for a checking function on the resultant data, subject to the protection of the identity of sources. It is not an all or nothing test. We would expect there to be few cases where judicious editing would not suffice to protect the competing public interest. This is recognised by the common law rules of natural justice. They acknowledge, for example, that a liquor licensing appellant should be entitled to know the gist of the case against him. As an additional safeguard, **we recommend below that the Privacy Commissioner should be entitled to review the matter and release data to the extent that prejudice is not likely.** We refer in our recommendation at paragraph 15.52(ii) to "statutory" bodies. We restricted our consideration to statutory bodies. There may well, however, be a need to extend the scope of this exception to non-statutory bodies at a later stage and this might be done by way of a schedule of specified bodies annexed to the legislation.

Judicial appointments

15.54 A category of appointments singled out by the United Kingdom Data Protection Act and not encompassed by the above categories relates to the judiciary. Section 31(1) of the UK Act exempts from the access provisions data received from third parties relevant to the making of judicial appointments. **We recommend a similar exemption.**

Legal professional privilege

15.55 Legal professional privilege is the legal principle which protects from disclosure in the course of legal proceedings communications with a legal adviser. This is more restricted than the general duty of confidence which subsists between solicitor and client (discussed in chapter 4) in that it is a rule of evidence that only arises in the course of legal proceedings. The fact that the privilege cannot be invoked in relation to other professional relationships reflects the singular importance that the common law attaches to ensuring the unrestricted communication between parties and their legal advisers. The United Kingdom legislature has taken a similar view in section 31(2) of the United Kingdom Act. **We recommend an exemption from the access provisions for data for which a claim for legal professional privilege can be made out.**

Confidential health and social work data

15.56 The United Kingdom legislation provides that access should be denied when serious harm is likely to be caused to the physical or mental health of the data subject. An additional ground is that the identity of a third party is likely to be deduced without his consent to its disclosure. Regarding this latter ground, it will be recalled that social work informants are thought deserving of the same protection as police informers (see Chapter 4).

15.57 We agree with the rationale of the first limb of the United Kingdom provisions, but think that it can be expressed in general terms and not specifically restricted to health or social work records. Accordingly, **we recommend that there be a general exemption to a right of access where access is likely to cause serious harm to the physical or mental health of the data subject.**

Access to evaluative data

15.58 In common with all data protection laws, we have recommended the regulation of all personal data, whether that data purports to be factual or evaluative. The distinction is often a matter of form and difficult to draw. Data protection laws are concerned with material upon which decisions are made affecting the individual. Evaluative data will often be more influential in this regard than factual data. There is the additional argument that people will be less prone to make sweeping assessments if aware that they may be scrutinised. Inger Hansen, former Canadian Privacy Commissioner, found that when collectors of information are aware of potential access, they "act more responsibly and fairly ... language becomes cautious [and] derogatory assessments will be supported by examples."[7]

---

[7] David Flaherty, Protecting Privacy is Surveillance Societies (University of North Carolina Press, 1989), page 271.

15.59 **Submissions on evaluative data** Several submissions expressed reservations about access rights to evaluative data generally. Respondents in this category include the Health and Welfare Branch, Planning, Environment and Lands Branch and the Hong Kong Institution of Engineers. The only arguments adduced for such a broad exclusion were that these evaluations reflect on their makers, that such data is "owned" by the data user, or simply the assertion that such a measure might "prove difficult." A more specific point is that one cannot "correct" an evaluation, a point we acknowledge. Although not articulated in any submission, there may also be the concern that access to such data could render those making the evaluation liable to defamation proceedings. It may be worth pointing out, therefore, that the defence of qualified privilege would protect disclosures made for legitimate purposes. This is dealt with in Chapter 18 on the media and data protection.

15.60 There was general support for access/correction rights to evaluative data evinced by the Consumer Council and the Bar Association. The Hong Kong Council of Social Services, among others, specifically supported access and correction rights to appraisals by employers. We consider that the application of access/correction rights to evaluative data more accords with principle and we reject any general access exemption for evaluative data. We consider such an exemption to be not only wrong in principle, but also to pose insurmountable operational problems. This follows from our earlier point that the distinction between "factual and "evaluative" data is largely a matter of form, as many evaluations purport to possess a factual basis. The opportunities for circumventing access requirements are obvious.

15.61 Whilst we reject a general access exemption for evaluative data, other submissions have persuaded us that such an exemption is required for the following specific categories of evaluative data.

15.62 **Credit scoring** Submissions from the banking sector opposed access to data disclosing their individual credit strategies, policies and risk tolerance. They do not wish to countenance data subjects taking issue over lending criteria. We understand that there is also concern that, if borrowers have precise knowledge of lending criteria, they may tailor their applications accordingly. The bank's competitive position may also be affected should other banks be apprised of their lending strategies. We acknowledge these concerns, but consider that there is a simpler answer than creating an additional exemption. In our view, such data would not constitute "personal data". Speaking more generally, general criteria do not constitute "personal data", whether they be employment criteria, credit criteria, or otherwise. Nor do they become personal data upon application to specific individuals. Indeed to hold otherwise would considerably swell the amount of data which would have to be provided to individuals applying for access. Nonetheless, the fact that the matter has been raised indicates that clarification is desirable. **We accordingly recommend for the avoidance of doubt that the statutory definition of "personal data" expressly exclude criteria of general application. Insofar as a decision may be expressed cryptically, the**

requirement that the data be provided in an intelligible form does not entail the decoding of the applicable criteria.

15.63 **Staff planning data** The submission of the Institute of Personnel Management specifically endorses "openness and encourages sharing individual appraisals [which] we consider important for positive employee relations". This accords with our own understanding of modern management practices, whereby apprising the individual of his relative strengths and weaknesses facilitates the positive modification of his behaviour. The submission also notes, however, that:

> *"In the scope of human resources management, some actions which serve business and planning purposes, such as retrenchment or redundancy in the case of consolidation, merging and reorganisation, must be effected promptly in response to changes in the business environment. As the use of this data is highly sensitive for individuals and groups of staff, any premature disclosure will certainly result in staff demotivation and have an adverse effect on staff relations."*

15.64 We accept this argument that access by the individual to second order decisions requiring interpretation may create more difficulties than it removes. Prematurely advising him of outcomes that may not eventuate may raise false hopes and dash expectations. Such data will often involve comparisons with other individuals and accordingly be exempt to this extent under our other proposals. More fundamentally, such data will reach the point where it relates more to the intentions of the organisation than to the individual. Insofar as it addresses long term plans, the data are subject to ongoing revision and do not pose an immediate threat to the individual's prospects. The United Kingdom Data Protection Registrar has commented that it was the intention of the Data Protection Act to exclude access to such data, but the resultant provision was too broad. He favours a specific narrow exemption to cover the situation. **We also recommend that staff succession planning data should be exempt from access and correction.**

15.65 **Interim access to decisional data** Several submissions raise the issue of whether interim access should be denied to data pertaining to the process of evaluating a final result. We think that a narrowly-drawn exemption is justifiable where interim access would hamper or inhibit the evaluative process. Access and correction rights would accrue, however, upon the decision's being made. **We accordingly recommend an exemption from interim access to data relating to an evaluative process which will be seriously disrupted by affording access before a decision has been made and where appeal rights exist. The data must be retained following the making of the decision, when access rights accrue.**

15.66 This exemption will be of limited application. Otherwise, it could conflict with a recommendation we make in Chapter 11 that prior to the

implementation of an adverse decision, the individual shall be provided an opportunity to correct the data that is the basis of the proposed decision.

15.67 **Expressions of opinion** The Labour Department queried whether expressions of opinion about a data subject sufficiently relate to that individual to constitute "personal data". We think they do and that the individual should have the opportunity to access and correct the attribution of opinions, including expert opinions. We note that the British Columbia legislation specifically includes expressions of opinion. We reject an access exemption to such data.

15.68 **Data relating solely to an individual as agent** One submission sought an exemption for data solely relating to an individual in his capacity as an agent of a company. The data would be restricted to that necessary to identify contact individuals in companies. We agree that it may be a fine line between data relating to an individual and that relating to a company. However, we think the safer course is not to create an exemption to this effect. This should not create a practical problem because, although the data purpose would need to be included in the exemption, the data protection principles would have little impact on the use of such data.

15.69 **Testimonials** An established category of data pertaining to pending decisions which are compiled in confidence are testimonials. They are dealt with below.

15.70 **The correction of evaluative data** We acknowledge that an evaluation cannot, strictly speaking, be corrected. At most the record can record the data subject's disagreement and any supporting reasons. We so recommend in Chapter 14.

15.71 **Confidentiality and access** The common law duty of confidence was discussed in Chapter 4. It limits the disclosure of information both factual and evaluative which is not publicly known and is entrusted to a person in circumstances imposing a duty of confidence. We commented on the similarity of the doctrine's content to that of the Use Limitation Principle. We concluded that with its rather different scope of application, the duty complements the protection to personal information provided by the Use Limitation Principle.

15.72 In the present context, the difficulty is that whilst the duty of confidence may complement the operation of the Use Limitation Principle, it may conflict with subject access rights. This conflict resides in the disparate policy aims of the two principles. Any *legal* conflict, however, is disposed of by giving access rights statutory effect. This follows from the basic legal principle that legislation overrides the common law:

> *"Where the defendant is compelled or authorised by statute to disclose confidential information, he may legitimately breach*

confidence, but only in respect of the information of which the statute requires disclosure."[8]

15.73 Access rights under a data protection law constitute such a statutory authorization to disclose confidential information pertaining to the individual seeking access, except insofar as such access rights are qualified. The issue accordingly arises whether access rights should be subject to an exemption regarding confidential material, and if so its scope. This requires balancing the two competing public interests involved, namely that confidences are respected and that individuals have access to data relating to them.

15.74 We are not aware of any data protection law that generally exempts data from access where the information was received in confidence. Some laws have very broad exemptions which could be capable of applying to confidential information, but they are not addressed to confidentiality as such. Our concern is that a broad subject access exemption to confidential data would possess the potential to fundamentally undermine the transparency and openness which access rights promote. We also recognise, however, that in some circumstances access to data disclosed in confidence may be harmful to the specific public interests over and above the general public interest that confidences be respected. We have recommended above detailed access exemptions where confidentiality is buttressed by additional public interest considerations. But we confirm the Consultative Document's rejection of a general exemption to subject access rights which focuses on the conditions of the data's transfer to the data user, namely that the information was provided "in confidence". In the light of submissions, however, we have had to consider a narrowly drawn exception to this principle for employment references.

15.75 **A general exemption for testimonials** In the Consultative Document we rejected a general exemption for employment references compiled on the condition of confidentiality. We recognised that individuals could feel inhibited in providing candid assessments if aware that access may be granted. On the other hand, we were concerned that recorded assessments may be erroneous or unfair and result in long term damage to the data subject's prospects. We noted that notwithstanding a specific exemption, it would remain possible for referees to furnish confidential testimonials denying access rights with the informed consent of the data subject. Also, an exemption would not affect oral assessments which are not reduced to recorded data, as the access rights would have nothing to fix onto. Instead of a general exemption for testimonials, the Consultative Document proposed an exemption from access/correction rights for evaluative or other data pertaining to appointments particularly affecting the public interest. The difficulty which we did not address was how such appointments were to be identified. We have abandoned that approach, the uncertain application of which was criticised by a number of respondents. Our revised

[8] Wacks, *op cit*, page 78.

recommendations should accommodate the concerns of many respondents, but they do not address testimonials relating to vacancies generally.

15.76 We have received a number of submissions arguing for a general access exemption for testimonials and references compiled in confidence. The Institute of Personnel Management addresses the issue as follows:

> *"While written references for employment are widely accepted as important information tools for decision making in the recruitment of staff, the proposed requirements, on the contrary, would discourage referees from providing a fair, unbiased and honest appraisal. The situation would be even worse if as a consequence of the legislation, verbal references replaced written references."*

15.77 We noted above the Institute's endorsement for open staff appraisals. We accept, however, that references are distinguishable. Unlike staff appraisals, they are compiled by those not under a duty to do so. It is arguable that without the assurance of confidentiality, potential referees will be disinclined to commit themselves in writing. We also note that the provision of confidential references is a well established practice, although we understand that a telephoned follow-up is common. Providing access rights to testimonials could be expected to increase reliance on oral assessments, thus vitiating the reality of such access rights. We are accordingly persuaded to provide an exemption to recognise this activity, but in terms that deny access only until the reference has fulfilled its purpose. **We accordingly recommend that access and correction rights be barred in respect of personal references supplied on a confidential basis by a person not under a duty to supply them to the organisation seeking to fill a vacancy. The exemption should cease to apply upon the position being filled.** This will ensure that such references will not become the basis of ongoing decisions about the individual without his being able to check and correct them. The prudent referee will ensure that the reference is either returned or destroyed. The importance of this has been highlighted by the recent House of Lords decision in *Spring v. Guardian Assurance and others* (Times Law Report, 12 July 1994) which held that a person giving a work reference for a former employee owed him a duty of care and could be liable to pay damages for negligence if the reference contained inaccuracies as a result of which the employee suffered damage.

15.78 It will be noted that the exemption in the previous paragraph only extends to employment references. It does not extend, for example, to credit references or educational references. The former are likely to be compiled by finance organisations and cannot be characterised as "personal" references. Academic references relating to an appointment would fall within the terms of the proposed exemption, but those compiled for other purposes would not. For example, the Hong Kong University raised the situation where it asks a school principal to submit a report on a pupil applying for entry. We

think this should be subject to access and correction rights, particularly in view of the long-term effects of such reports on the life chances of the data subject.

Indirect access through data protection authority

15.79 Under the United Kingdom system the data user decides in the first instance whether access is likely to prejudice the purpose, except in the case of its national security and health data where others are involved. A data user's decision can be investigated by the Registrar. We prefer the system adopted in a number of European jurisdictions which provides for indirect access through the data protection authority. In France, for example, indirect access is provided for data pertaining to national security, defence, and public safety. Upon application from the data subject, a judicial member of the data protection authority reviews the entire file. Similarly, the German Data Protection Commissioner can examine security and police files on behalf of individuals and release selected data to them. This approach is endorsed by article 14 of the draft Directive. This provides for exemptions of the type of data purpose dealt with above, but adds that nonetheless "the supervisory authority shall be empowered to carry out the necessary cheeks, at the data subject's request, so as to verify the lawfulness of the processing within the meaning of this Directive."

15.80 We endorse this mechanism of indirect access. The independent review of the release of security and police data is viewed in France and Germany as an important protection of civil liberties. Aside from the special case of data certified by the Governor as relating to security, defence, or international relations (dealt with below), we consider indirect access as a necessary control mechanism of general application to all access exemptions. The mechanism is opposed by the HKMA but supported by the Bar Association. **We recommend that except in the case of data held for security, defence or international relations purposes in respect of Hong Kong, the Privacy Commissioner shall upon application review the release of data where the data user has claimed an access exemption.** However, we emphasise that the initial responsibility in fully responding to access requests lies with the data user. **We therefore also recommend that the statutory language make it clear that access requests should be complied with insofar as it is possible to do so without prejudicing the exempted purpose.**

Security in respect of Hong Kong

15.81 This interest raises exemption issues both in relation to the Use Limitation Principle and access and correction rights. It is dealt with at this stage because our recommendations on this aspect depart in some respects from the scheme recommended above.

15.82 Section 27 of the United Kingdom Act provides that personal data are exempt from registration requirements and subject access and

correction provisions "if the exemption is required for the purpose of safeguarding national security." A certificate signed by a minister "certifying that the exemption is or at any time was so required shall be conclusive evidence of the fact." Although the exemption does not in terms extend to the non-application of the data protection principles, this is the practical result. This is because under the United Kingdom Act only registered data users are subject to an enforceable duty to comply with the principles. Under our proposals, however, the application of the principles is not dependent on compliance with the administrative requirement of lodging a declaration.

15.83 Although individuals are accordingly denied any redress under the United Kingdom Act in respect of the misuse of data subject to the exemption, the Security Service Act 1989 affords limited redress to individuals aggrieved by the activities of MI5, the UK's domestic security service. The Act establishes a tribunal of lawyers to investigate complaints. It follows that in the United Kingdom security service outsiders are now conferred a general supervisory role. They do not, however, specifically monitor the application of the data protection principles to the collection and use of security-related data.

15.84 In the Consultative Document we made the following general points regarding this provision:

(i) Lack of definition

"National security" is undefined in the legislation. While it is also undefined in section 1(2) of the United Kingdom Security Service Act 1989, that provision gives as examples protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means. "National Security" was considered by Lord Justice Lloyd in his 1989 Annual Report under the Interception of Communications Act 1985, an enactment which also does not define the term. He concluded that it was narrower than the "public interest" and wider than counter-terrorism, counter-espionage and counter-subversion. He did not think it possible to define it more closely than this and that "each case must be judged on its merits." If this is accepted, there is a discretionary element in determining the ambit of the interest to be protected. A related point is that a number of situations may readily be subsumed under both this interest or a related one, such as law enforcement. An example would be a serious riot.

(ii) Impact on ordinary individuals

Related to the possible width of "national security" is the potential for the purpose to impinge on ordinary individuals. Security vetting figures in the United Kingdom refute the notion that national security data uses relate to a clandestine minority. The security service plays a decisive role in the security vetting of some 770,000 appointments. Some 66,000 sensitive posts are subject to positive vetting, whereas the

remainder undergo negative vetting (the "nothing known against" procedure).[9]

(iii) Exemption relates to data purpose

In common with the other exemptions under the UK Act (and also our own recommendations), the exemption arises from the use of the data, and not from the identity of the holder of the data as such. Thus the exemption is expressed to pertain to data "if the exemption is required for the purpose of safeguarding national security." This is a question of fact regarding the use of the data in question, and not merely whether it is held by the security service.

15.85 **Submissions on the exemption for data in respect of the security of Hong Kong** The Hong Kong Human Rights Commission commented:

> *"Some sensitive data is kept by the government, for example, name list and background of individual persons kept by Special Branch, membership lists of registered organisations, and personal data recorded by the police in rallies. The government has not specified where the data is stored, what its purposes are, how long it will be stored and whether it will be transferred to another party or destroyed. The quantity of such data is also unknown.*
>
> *If the data enjoying exemptions mentioned in the Consultative Document also includes the above mentioned data, correction cannot be made by involved individuals when there are mistakes. The general public or organisation members cannot check if their data has been stored in it. We therefore suggest that exemption should not be granted to such sensitive data."*

15.86 **Recommendation on data held for national security purposes** We put international relations and defence in the same category as security in respect of Hong Kong. We note that the three interests are all explicitly addressed in the United Kingdom Official Secrets Act 1989 and, locally, the Commissioner for Administrative Complaints Ordinance (Cap 397). On the other hand, the UK Data Protection Act exemption only refers to "national security". This could be attributable to the analytically distinct concepts of "defence" and "international relations" being subsumable under the vague rubric of "national security". We have noted the Bar Association's submission that "defence" be deleted as a separate heading but, although there will be overlap situations, we consider it to refer to a distinct interest and reject this submission.

15.87 **We recommend that data held for the purpose of security, defence and international relations in respect of Hong Kong should be**

---

[9] R. Norton-Taylor, *In Defence of the Realm?* (London, The Civil Liberties Trust, 1990), pages 72-3.

exempted from access and correction rights and from the application of the Use Limitation Principle whenever that interest is likely to be otherwise prejudiced. A certificate signed by the Governor or Chief Secretary would be evidence of the exemption. Data users would nonetheless remain subject to the general requirement to furnish declarations describing in general terms the data held for these purposes. The other data protection principles would apply. As regards the data identified in the certificate, the Privacy Commissioner would be entitled to look behind the certificate of the Governor or Chief Secretary to confirm that the data purpose for which the exemption was claimed was correctly classified as relating to security, defence or international relations in respect of Hong Kong. This latter feature goes further than the United Kingdom provision. This is thought necessary because of the constraints imposed in Hong Kong by the Bill of Rights, which has no UK counterpart. Our recommendation also addresses concerns raised by the Hong Kong Human Rights Commission. As indicated above, an exemption under this ground is broader than those applying to related interests, such as law enforcement, as even indirect access through the Privacy Commissioner is barred. It is accordingly important that the Privacy Commissioner can check that data are not unnecessarily being ascribed to this ground when a more mundane classification would suffice. We note, in this regard, the Canadian Privacy Commissioner's comment that he had "occasionally been able to determine that a government institution had incorrectly withheld information from an applicant as the information was not even of the type covered by the exempting provision".

15.88 In performing his checking function to determine that the data have been correctly classified as relating to national security, defence, or international relations in respect of Hong Kong, the Privacy Commissioner must necessarily have access to all the data. Insofar as this is thought to raise security questions, we are advised by senior Canadian officials that this arrangement has not created security problems in that country, access being restricted to the Privacy Commissioner or his deputy.

15.89 **No indirect access to security data** The further question arises of whether in addition to determining whether the data are correctly classified the Privacy Commissioner should be entitled to review the certificate's assertion that the data is required for the purpose of security, defence or international relations in respect of Hong Kong. Should he conclude that it was not so required it would follow that the exemption was not made out and the data should be released. The Consultative Document proposed that the Privacy Commissioner should not be able to look behind the Governor's certificate on this factual question. The Bar Association criticised this denial of indirect access as providing a somewhat restrictive role for the Privacy Commissioner. It suggested that he should be entitled to determine, in the light of the certificate, not only whether the data is correctly classified, but also that allowing subject access would be likely to prejudice the stated interest. It would follow that should he determine that prejudice is not likely, the data should be released. The submission notes that this system

of indirect access applies to all the other access exemptions we have recommended.

15.90 Regarding this issue, we note that article 15 of the draft Directive provides that access exemptions may be conferred in respect of various public interests, including national security and defence. It further provides, however, that as regards such data:

> *"the supervisory authority shall be empowered to carry out the necessary checks, at the data subject's request, so as to verify the lawfulness of the processing within the meaning of this Directive."*

15.91 Having further considered the matter, we have decided to adhere to our earlier proposal, whereby the Privacy Commissioner's checking function is restricted to confirming that data referred to in the certificate are correctly characterised as relating to security, defence or international relations. We note that unlike the other exempted interests, the assessment of likelihood of prejudice will be in the form of a certificate by the Governor or Chief Secretary. Nonetheless, we recognise that safeguards are required. The Consultative Document recommended that this take the form of adopting a complaints mechanism regarding the activities of the security service along the lines of the United Kingdom Security Service Act 1989. However, that legislation does not provide for the independent scrutiny of security service databases, nor does it extend to defence or international relations. We have accordingly abandoned that proposal. Instead, we recommend the following additional safeguards:

(i) *Monitoring role of Privacy Commissioner.* The Consultative Document, proposed that apart from access/correction rights and the Use Limitation Principle, the other data protection principles should apply to data relating to security, defence, or international relations. It did not, however, draw the corollary that the Privacy Commissioner would be able to monitor compliance with the data protection principles. This is not consistent, particularly since we recommend that he have access to all relevant data. **We therefore recommend that upon receiving a complaint, the Privacy Commissioner should be entitled to monitor compliance with the principles. However, in responding to the data subject, the Privacy Commissioner will only indicate that he has made all necessary inquiries and will not disclose whether there is a file on the inquirer. This will preclude the complainant from pursuing any appeal to the tribunal.** Instead, he would be dependent on the Privacy Commissioner pursuing any concerns he has about compliance with the principles or the use of the exemption by reporting the matter to the Governor and/or the Legislative Council.

(ii) *Revision of the matter to be certified by the Governor.* The Consultative Document adopted the United Kingdom formulation of certifying that the exemption is "required" for the purpose of safeguarding security. This test would appear to be less objective than the test we have adopted for our other exemptions, namely that of likelihood of prejudice to the competing interest. Our revised recommendation accordingly adopts the likelihood of harm test in this context also.

COE recommendations on police data

15.92 The Council of Europe has promulgated a detailed set of recommendations regulating the use of personal data in the police sector[10]. To a large extent, these detailed recommendations are encompassed by the application of the data protection principles. In some respects, however, they go further than a literal application of the principles would suggest. For example, they are more emphatic that data should be deleted when it is no longer necessary for its original purpose. Also, being a sectoral code, it usefully highlights salient issues arising from this data purpose. We consider that it usefully supplements the general data protection provisions we have recommended. **We recommend that the Council of Europe recommendations regulating the use of personal data in the police sector should be used as the basis for devising a similar code suitable for Hong Kong.**

The media

15.93 Article 16 of the BOR provides for the protection of freedom of speech which is an important right in a free society. Free speech as exercised by the media plays a fundamental role in the respect for human rights generally, by informing public opinion of possible abuses. The difficulty is determining where to draw the line between the exercise of freedom of expression and the potentially competing data protection principles. This complex issue is now separately addressed in Chapter 18.

The Collection Limitation Principle

15.94 It will be recalled that this provides:

> *"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."*

[10] Council of Europe, *Regulating the Use of Personal data in the Police Sector,* (Strasbourg 1988).

15.95 The collection of data by means of "tip-offs" has been dealt with above in connection with the exemptions from the Use Limitation Principle. Some of the submissions also refer to activities such as surveillance and seek any necessary exemptions from this principle. The words "where appropriate" have the potential to sanction such activities, but determining this will constitute a major exercise in its own right. The second part of our reference will provide the opportunity to fully examine the circumstances when this principle may be departed from to conduct surveillance, intrusion and the interception of communications. We are not in a position to recommend detailed exemptions from this principle at this stage.

Chapter 16

Structure, functions and powers of the Privacy Commissioner

Summary

16.1 If the detailed regulatory framework governing the use of personal data we have recommended in previous chapters is to be effective, we think it essential that an authority with powers to ensure compliance be established. Most countries with data protection laws have established such bodies. We propose the establishment of such an authority, which we refer to as "the Privacy Commissioner".

16.2 Investigation of complaints by the Commissioner assists data subjects to enforce their rights and means that litigation need only be resorted to for appeals or judicial review.

16.3 This chapter examines the structure, functions and powers appropriate for the Privacy Commissioner. We think the Privacy Commissioner should have an investigative role and be assisted in policy formulation by a board.

16.4 We consider the independence of the Commissioner is fundamental. This requires adequate safeguards in the making of appointments, security of tenure for those appointed, and a budget sufficient to fulfil the authority's functions effectively.

16.5 We believe that the Commissioner should not be restricted to responding to complaints but should be able to initiate his own investigations and on-site inspections.

16.6 Data users will have to provide the declarations described in previous chapters to the Commissioner. The Commissioner will approve sectoral codes of practice and publicise data protection requirements.

16.7 We believe that powers to enter premises and obtain evidence are necessary to enable the Commissioner to carry out his functions. The data user's consent should first be sought but, if that is not forthcoming, the court should be empowered to make an appropriate order for entry and seizure.

16.8 We consider that disputes between data subjects and data users should be referred to the Administrative Appeals Board.

Recommendations

16.9 Overseeing observance of the regulatory requirements of a data protection law should be the sole responsibility of an independent authority established for the purpose. In addition to assisting individuals to enforce their rights, the authority should perform a number of other functions, including the investigation of complaints, the provision of a central notification point for data users furnishing declarations describing their personal data systems, the conduct of on-site verifications regarding the operation of such systems, and the carrying out of educational and publicity functions. The authority is referred to as the "Privacy Commissioner" (paragraphs 16.40-41).

16.10 The full-time Privacy Commissioner should be assisted in the formulation of policy by a board of five part-time members of high standing representing the public and private sectors with not more than one government servant and at least one member having extensive experience in data processing. There should be no maximum age limit. The board of commissioners should meet not less than quarterly (paragraph 16.44).

16.11 The Privacy Commissioner and the commissioners should be appointed by the Governor. The Privacy Commissioner should be appointed for a term of five years with the option of not more than one further appointment. Part-time commissioners should be appointed for a term of three years, with the option of not more than two further appointments (paragraph 16.46).

16.12 The tenure of the Privacy Commissioner should be protected by a provision requiring that he may only be removed from office by the Governor with the approval by resolution of the Legislative Council on the ground of inability to discharge the functions of office, or misbehaviour. Members of the board of commissioners may be dismissed by the Governor alone (paragraph 16.48).

16.13 To secure an adequate budget, a levy of $100 should be levied on all applicants for business registration (paragraph 16.51).

16.14 The Privacy Commissioner should have the following functions:

(a) investigation of complaints;

(b) the conduct of on-site inspections of data users;

(c) notification point for declarations from data users;

(d) promoting codes of practice; and

(e) educational and publicity functions (paragraph 16.52).

16.15 The Privacy Commissioner should investigate any complaint that any of the data protection principles or provisions of the data protection law have been, or is being, contravened (paragraph 16.55). He should be expressly empowered to initiate investigations in the absence of a complaint, provided he has reasonable grounds for suspecting a breach of the data protection law (paragraph 16.66).

16.16 The Privacy Commissioner should have a limited discretion to decline to investigate complaints on well-established grounds regarding lack of merit (paragraph 16.55).

16.17 Data subjects should have the right to complain direct to the Privacy Commissioner (paragraph 16.57). Complaints should be reduced to writing. The Privacy Commissioner should be under a duty to assist persons in formulating a complaint, but should not intervene unless assistance is requested (paragraph 16.58).

16.18 There should be provision for class complaints along the lines that, in the case of an act or practice that may be an interference with the privacy of two or more individuals, any one of those individuals may make a complaint (paragraph 16.59).

16.19 The Privacy Commissioner should have the discretion to regulate his own procedures, subject to safeguards regarding fairness. The respondent should be informed at the outset that a complaint against him has been received. The Privacy Commissioner should be able to hear or obtain information from such persons, and make such inquiries, as he thinks fit. A person should only be entitled to be heard by the Commissioner if the Commissioner is proposing to make an adverse report or recommendation on him (paragraph 16.60).

16.20 When a hearing is necessary, it should be held in public unless the data subject requests otherwise, in which case the hearing should be in private (paragraph 16.62). In the course of a hearing, counsel and solicitors should not have any right of audience before the Commissioner, but may appear before him if he thinks fit. The discretion should explicitly extend to lay representation (paragraph 16.63).

16.21 The Privacy Commissioner should inform both parties in writing of the result of his investigation. Should he exercise his discretion and decline to conduct an investigation, or to take enforcement action following investigation, he should advise the complainant in writing of his decision or opinion and his reasons (paragraph 16.64).

16.22 Data subjects may judicially review (but should not have the right to have reviewed on its merits) a decision of the Privacy Commissioner not to investigate a complaint or not to take enforcement action following an investigation (paragraph 16.65).

16.23 Upon finding a complaint substantiated, the Privacy Commissioner should be empowered to direct the remedy of the breach in a specified manner. The data user's Responsible Officer should be subject to a duty to notify the Commissioner that compliance has been effected. Failing compliance, the Commissioner should seek an enforcement order in court. If compliance with the data protection principles cannot be adequately secured by an enforcement order, the Privacy Commissioner should apply to the court for an order prohibiting the organisation from processing personal data (paragraph 16.67).

16.24 A right to compensation should accrue from any breach of the data protection principles causing loss or injured feelings (paragraph 16.70). The Privacy Commissioner's role in compensation claims should be limited to determining whether there has been a breach of the principles. Upon his so certifying it should be for a court to determine the appropriate amount of compensation payable, if any. The status of the certificate in the court proceedings will be that of *prima facie* evidence, rebuttable on the balance of probabilities (paragraph 16.72).

16.25 The Privacy Commissioner should have the power to initiate systematic on-site inspections of personal data systems. The purpose of the power would be to check that the data protection principles are being complied with and that appropriate control systems are in place. This should include verifying the accuracy of the organisation's declaration and extend to a physical examination of the operational adequacy of such aspects as storage security (paragraph 16.76). It should be expressly provided that the power be exercised in a manner that does not unduly disrupt the organisations daily operations. The board of commissioners should approve the schedule of data users selected for on-site inspections (paragraph 16.77).

16.26 The Privacy Commissioner and his staff should be subject to a legal duty of secrecy subject to criminal sanctions (paragraph 16.78).

16.27 The Privacy Commissioner should not be required to approve data uses described in declarations. The extent of his legal duty in responding to declarations should be to store them in a publicly accessible form. He should be empowered, however, to require further and better particulars when he sees fit (paragraph 16.82).

16.28 Where a prosecution follows an offence under the data protection law, summary offences should face a maximum fine of $50,000. Indictable offences should face an unlimited fine as well as the destruction or amendment of the off ending data (paragraph 16.83). The Privacy Commissioner should be required to compile an annual report to the Governor which should also be laid before the Legislative Council (paragraph 16.84).

16.29 Where in the exercise of his functions the Privacy Commissioner requires entry to premises, the following procedures should be adopted:

(a) where entry is not urgent, the Commissioner should initially approach the organisation's Responsible Officer. If consent is not forthcoming at that stage, the Commissioner should serve a notice advising that if consent is not received within 14 days then he will seek a court order and apply for costs (paragraph 16.86).

(b) where entry is urgent, the Commissioner should approach the court forthwith, thereby dispensing with the 14 day grace period. In such cases, the Commissioner will consider it inadvisable to alert the organisation to his imminent visit (eg to avoid the destruction of evidence) and he should be empowered to approach the court direct for an order along the lines of an *Anton Piller* order authorising entry and seizure (paragraph 16.87).

16.30 The Privacy Commissioner should be empowered to serve notice on any person requiring that person to furnish in writing such information or to produce any document or thing as is necessary or expedient for the performance of the Commissioner's functions. Such a notice should be appealable to a court. The necessary legal provisions should also address such ancillary matters as over-riding secrecy provisions, limiting the use of answers in other proceedings, and restrictions where it is certified that public interests such as national security may be prejudiced (paragraph 16.89).

16.31 The Privacy Commissioner should be empowered to seize any material, whether or not it may be subsequently ascertained that it is subject to an exemption, provided that he has reasonable cause to suspect that the data protection law has been contravened in respect of some of its contents and that any exempt data are returned within a reasonable period (paragraph 16.90).

16.32 The Privacy Commissioner should not be empowered to obtain evidence on oath, but it should be a criminal offence to wilfully make a false statement to the Commissioner (paragraph 16.91).

16.33 The Privacy Commissioner's decisions should be subject to judicial review. There should also be a right to appeal on the merits of decisions made by the Privacy Commissioner. Such appeals by data users and data subjects should be considered by the Administrative Appeals Board (paragraph 16.92).

The need for an independent authority

16.34 In only one country is the regulation of the data protection principles left to the data subject, unaided by an independent data protection authority. The USA lacks a supervisory body specifically constituted to oversee compliance with the data protection requirements contained in its 1974 Privacy Act. A limited regulatory role has been assigned to the Office of

Management and Budget, but it does not assist individuals to enforce their rights. Instead, individuals have to bring lawsuits in the courts. Requiring individuals to sue for breaches of privacy has a number of drawbacks. Some of these are inherent in any litigation. The high cost of litigation tends to deter ordinary individuals from pursuing claims. In addition, delays commonly characterise the conduct of litigation and figures indicate that this is true of US privacy claims.[1]

16.35 Other drawbacks in requiring individuals to sue for privacy violations derive from the nature of the right in question. Such proceedings may well entail a traumatic abandonment of privacy in order to remedy its infringement. Nor are damages, the primary remedy of civil proceedings, often the most appropriate means of such redress. Nonetheless, we note that many data protection acts include provisions for civil redress and we similarly recommend below. However, whilst such provision may be useful as a supplement to an independent data protection authority, we consider that sole reliance on civil remedies affords data subjects inadequate protection.

16.36 In addition to assisting data subjects to uphold their privacy rights, ensuring an effective data protection regime requires a government body to exercise a general monitoring role. In the USA this role is performed by the Office of Management and Budget. This is part of the Executive Office of the President and has been described by Flaherty as lacking sufficient independence from the political process to enable it to vigorously pursue privacy protection.[2] We take the point that privacy interests will often conflict with the immediate operational aims of government departments. Effective data protection requires a truly independent body specifically charged with the task of ensuring compliance.

International instruments on the need for an independent authority

16.37 International instruments dealing with data protection have recently specifically addressed the need for a supervisory authority. Article 30(1) of the draft Directive provides that:

> *"Each Member State shall designate an independent public authority to supervise the protection of personal data. The authority shall be responsible for monitoring the application of the national provisions taken pursuant to this Directive and for performing all the functions entrusted to it by this Directive."*

16.38 It will be recalled from Chapter 4 that the terms of the Hong Kong BOR are based on those of the ICCPR. Whilst the privacy provision of the BOR does not explicitly require an independent supervisory authority, the Human Rights Committee's elaboration on the corresponding ICCPR

---

1 David Flaherty, *op cit*, page 343.

2 David Flaherty, *ibid,* page 325.

provision articulates access and correction rights necessitating specialised administrative expertise (see Chapter 2). This issue has now been specifically addressed by the 1990 United Nations Guidelines for the Regulation of Personal Data Files. The ICCPR was also promulgated by the United Nations, and although the guidelines are not explicitly an elaboration on the ICCPR provisions, they were formulated with reference to those provisions. The guidelines would accordingly constitute persuasive authority as to the interpretation of the ICCPR, and hence the BOR. Principle 8 of the UN Guidelines provides that:

> *"The law of every country shall designate the authority which, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles set forth above. This authority shall offer guarantees of impartiality, independence vis-a-vis persons or agencies responsible for processing and establishing data, and technical competence. In the event of violation of the provisions of the national law implementing the aforementioned principles, criminal or other penalties should be envisaged together with the appropriate individual remedies."*

Human Rights Commission a separate issue

16.39 For completeness, we should add that we consider the arguments justifying the establishment of a data protection authority to be distinct from and additional to those in respect of setting up a body with a general human rights oversight role. The provisions of the BOR are cast in extremely wide terms, with the privacy provision consisting of two sentences. By way of contrast, the recommendations contained in this document constitute a highly detailed regulatory scheme. To this extent a data protection authority would have a far more specific role than that of overseeing the BOR generally. As this issue raises different considerations outside our terms of reference, we express no opinion on the matter.

Recommendation on independent authority

16.40 It follows from the above that there are strong arguments in principle, as well as practical considerations, supporting the establishment of a regulatory authority. **We accordingly recommend the establishment of an independent authority tasked to monitor compliance with the regulatory framework we propose.** In addition to assisting individuals to enforce their rights, the authority will perform a number of other functions which we consider essential to the adequate regulation of personal data. They comprise the investigation of complaints, the provision of a central notification point for data users furnishing declarations describing their personal data, the conduct of on-site verifications regarding the operation of such systems, and the carrying out of educational and publicity functions. These functions are described in detail later in this chapter. For convenience,

we shall refer to the proposed data protection authority as the "Privacy Commissioner". We do not intend by this, however, to preclude the use of a different title if this is thought more appropriate at a later stage.

Structure of the authority

Independence of the Privacy Commissioner

16.41 Authorities established in other jurisdictions differ in their structure. All are headed by a chief executive designated as "Privacy Commissioner", "Data Protection Commissioner" or similar. Usually he or she is fully in charge of implementing data protection measures. An exception is Canada. There, the Federal Privacy Commissioner's role in implementing data protection is shared by the President of the Treasury Board, the designated minister concerned with privacy for most administrative purposes. This arrangement reflects a conscious decision on the part of the government to retain ultimate responsibility under traditions of Cabinet government. Flaherty has described this sharing of an oversight role as "an open invitation to weak implementation."[3] Also, the constitutional argument in favour of this arrangement in Canada is less relevant in Hong Kong. **We accordingly recommend that the Privacy Commissioner should be independent and should be fully responsible for the implementation of a data protection regime in Hong Kong.** By "independent" we mean that the Commissioner should not be brought under the wing of the relevant policy department. The Privacy Commissioner must be independent of the executive to protect his role from being usurped by a sector he has the duty of regulating. Instead, he should have a role analogous to that of the Commissioner for Administrative Complaints or the Electoral Boundaries Committee.

Board of commissioners

16.42 There is less agreement among other jurisdictions on whether the Privacy Commissioner should be assisted by a board of advisors or commissioners. In the United Kingdom, for example, the Data Protection Registrar is assisted by his Deputy and Assistant Registrars, but not by a board of advisors. In France and Sweden, on the other hand, the chief executive is assisted by a board or commission. The Swedish Data Inspection Board comprises eleven part-time members representing various political parties and interest groups to advise on basic policy. The French agency is run by a commission of seventeen part-time members of a similarly diverse composition, but unlike the Swedish body they also involve themselves in day-to-day operational decisions.

16.43 We believe a board of part-time commissioners could usefully assist the Privacy Commissioner in the formulation of policy. As we envisage an investigative role for the Privacy Commissioner, it lessens the potential for

[3] David Flaherty, *op cit*, page 250.

conflicts of interest that could arise if he was solely responsible for the formulation of the policies he is to apply. The day-to-day operational and investigative decisions should be left to the Privacy Commissioner and his full-time staff, subject to the limited monitoring role we refer to at paragraph 16.45.

16.44 **We therefore recommend the establishment of a board of part-time commissioners consisting of five persons of high standing representing the public and private sectors with not more than one government servant and at least one member having extensive experience in data processing.** A board of five members provides, we think, a variety of perspectives without being unwieldy. **We also recommend that a maximum age limit is not appropriate. There should be a requirement that the Board meet not less than quarterly.** An independent secretariat to service the Board would be desirable.

16.45 Professor Colin Bennet and Mr Thomas Riley, both international authorities on data protection, criticised our recommended board of part-time commissioners. We are aware that only Sweden and France have such a system. Professor Simitis was also critical, saying that such an approach had proved a failure in a German province. However, we disagree with the suggestion that in Hong Kong it would lapse into a cosy arrangement lacking adequate commitment. On the contrary, we think the board would provide a useful system of checks and balances in a society where part-time boards have proved an essential element of administration. The board would be subject to the scrutiny of the Legislative Council and the public. The board could provide a buffer zone of support for the Privacy Commissioner, instead of the latter being the sole focus of adverse pressures. It would be the Privacy Commissioner, however, who would assume the overall leadership role. Nonetheless, we envisage that the board should have a limited role in monitoring the Privacy Commissioner in the exercise of his power to initiate inspections of personal data systems. We elaborate on this in paragraph 16.77.

Appointment of the Commissioner and board of commissioners

16.46 We have recommended above that both the public and private sectors be regulated. To avoid potential conflict of interest situations, it is essential that the agency be as independent as possible. Appointment procedures for the posts of Privacy Commissioner and the part-time commissioners should be suitable for this purpose. In other jurisdictions this has been achieved by making the Commissioner answerable to the legislative assembly. One possibility was to make the appointment by a vote by LegCo on a proportional basis, but this carries the danger of politicisation of the selection process. The Consultative Document proposed that appointment of the Privacy Commissioner and the commissioners be by the Governor on the advice of the President of the Legislative Council. This would be an unusual procedure and we have doubts as to whether such a system is feasible. We prefer that the appointment be made by the Governor but that in carrying out that task the Governor should seek advice from others in the community,

including perhaps the President of the Legislative Council. **We accordingly recommend that the Privacy Commissioner and the commissioners be appointed by the Governor. The Privacy Commissioner should be appointed for a term of five years with the option of not more than one further appointment. Commissioners should be appointed for a term of three years, with the option of not more than two further appointments.**

16.47 Our Consultative Document did not attempt to identify appropriate qualifications for the Privacy Commissioner and this was subject to some criticism. Having further considered the matter, however, we have been unable to specify precisely either positive requirements (such as legal qualifications) or negative factors precluding appointment (such as that he not be appointed from the civil service). Nor do we agree with the suggestion that at least one member of the board must be a lawyer. We envisage that the Privacy Commissioner's office will have its own legal staff.

16.48 Once appointed, security of tenure is necessary to ensure continued independence. The Commissioner for Administrative Complaints Ordinance (Cap 397) establishes a post which, like that of the Privacy Commissioner, will necessarily involve querying administrative action. The incumbent's tenure is therefore secured by section 3(4)(a). This provides that he may only "be removed from office by the Governor with the approval by resolution of the Legislative Council on the ground of inability to discharge the functions of his office, or misbehaviour." **We recommend a provision in similar terms to protect the tenure of the Privacy Commissioner. We do not think this procedure would be unduly cumbersome as regards members of the board of commissioners and recommend that they may be dismissed by the Governor alone.**

Financial provision

16.49 In addition to independent appointees, an enforcement agency's independence is dependent on an adequate budget. Lack of funding could throttle the agency's effectiveness. Public expenditure is increasingly scrutinised nowadays, but adequate data protection expenditure represents value for money. In Germany, for example, concern was expressed about the cost of running a Federal agency with a staff of just over thirty. The Data Protection Commissioner responded that there is hardly any other area of public administration that can achieve such a relatively large effect with such comparatively limited resources, his 1980 office budget being less than the printing and distribution costs of the Federal budget.[4] To the same effect, his successor pointed out that his office budget was less than one percent that of the cost of electronic data processing by the Federal Government.[5]

16.50 An indication of the cost of regulating both the public and private sectors in Hong Kong is provided by the 1992 annual report of the UK Data Protection Registrar. In the 1991/2 financial year he received government

[4] David Flaherty, *op cit*, page 55.
[5] David Flaherty, *op cit*, page 42.

grants of £3,423,094. Registration fees provided £2,254,965. Operating costs, including salaries, totalled £3,308,683. The United Kingdom has a population of approximately 58 million compared with Hong Kong's approximate 6 million.

16.51 In Chapter 10, we recommend that the principal means for identifying relevant holders of personal data and bringing them within the scope of regulation should be the Business Registration scheme. There are over 600,000 registered businesses in Hong Kong. The current annual registration fee is $2,000. **We recommend that an additional levy for data protection funding on a cost recovery basis be imposed on all registering businesses, whether or not they hold personal data.** We expect the majority of registering businesses will hold personal data. The recommendation should remove a minor incentive to not report doing so. **On the basis of the UK figures, a fee of not more than $100 would fully cover the operating costs of the Privacy Commissioner.**

Functions of the Privacy Commissioner

16.52 **We recommend that the data protection authority have the following functions:**

(i) investigation of complaints;

(ii) the conduct of on-site inspections of data users;

(iii) notification point for declarations from data users;

(iv) promoting codes of conduct; and

(v) educational and publicity functions.

16.53 Before examining these functions in detail, a general point may be in order. The UK Act fails specifically to identify all the Registrar's various functions. We prefer the more explicit approach adopted by other legislation in the area. The Australian Act, for example, separately itemises 13 different (but sometimes overlapping) functions.

Investigation of complaints

16.54 A function common to almost all data protection agencies is the investigation of complaints of contravention of the data protection principles. Recent annual reports from other jurisdictions illustrate the range and volume of complaints. For the year ending June 1992, the UK Registrar reports having received 1,747 complaints, down from the previous year's 2,419. Consumer credit data complaints accounted for 32%, followed by complaints about direct mail (18.5%), unfair obtaining, subject access (percentages for

these two categories not specified), and non-registration (4%).[6] The Australian Act covers a much smaller population and focuses on the public sector. For the year ending June 1992 the Australian Privacy Commissioner received 220 complaints falling within his jurisdiction. The most frequently cited processing complaint related to limits on use and disclosure.

16.55 **Scope of duty to consider complaints** The subject matter of complaints should be widely drawn. Section 36 of the UK Act Data protection provides that a complaint may be entertained where "any of the data protection principles or any provision of this Act has been or is being contravened." **We recommend the adoption of a similarly broad formula.** However, data protection laws do not usually impose on the Privacy Commissioner an unconditional duty to investigate all such complaints, but instead confer a limited discretion in the matter. Limitations may be implied by the formulation of the scope of the duty. For example, section 36(2) of the UK Act requires the Registrar to consider a complaint "if [it] appears to him to raise a matter of substance and to have been made without undue delay by a person directly affected." Alternatively, the law may impose a general duty, but identify various grounds negating the duty, such as the fact that the complaint appears to be frivolous or without merit. This latter approach is adopted by section 41 of the Australian Privacy Act and, in Hong Kong, by the Commissioner for Administrative Complaints Ordinance (Cap 397). Whichever drafting approach is adopted, **we recommend that the Privacy Commissioner have a limited discretion to decline to investigate complaints on well-established grounds regarding lack of merit. These should be narrowly drawn, however, because we understand from overseas authorities that it is difficult to ascertain at the outset whether a complaint has substance.**

16.56 **False complaints** We considered whether it should be an offence to make a false complaint. We understand, however, that this has not proved a problem in other jurisdictions, even if a subjective element will often motivate the making of the complaint. We accordingly do not recommend such a provision.

16.57 **Direct access** The comparatively specialised nature of data protection requires that data subjects should have direct access to the enforcement agency. A referral system such as was hitherto in place for the Commissioner of Administrative Complaints would be unworkable in this area. We note that there is now direct access to the Commissioner. There is also direct access to the UK Data Protection Registrar. **We accordingly recommend that data subjects have the right to complain direct to the Privacy Commissioner.**

16.58 **Form of complaints We recommend a requirement that complaints be reduced to writing. The enforcement agency should be under a duty to assist persons in formulating a complaint, but should not intervene unless assistance is requested.** An assistance requirement

[6] Eighth Report of the Data Protection Registrar, June 1992, London: HMSO.

is not contained in the UK Act, but is provided for in the Australian Act, for example.

16.59 **Class complaints** We understand from discussions with overseas data protection officials that meritorious complaints usually throw up defective data handling practices whose adverse effects are not restricted to the complainant. Carol Wallace of the Quebec authority pointed out that privacy problems are systemic, likening them in this respect to environmental problems. Complaints tend to highlight concerns of a general nature relating to the processing of personal data. In recognition of this, **we recommend that there be provision for class complaints along the lines of section 36(2) of the Australian Act. This provides that "in the case of an act or practice that may be an interference with the privacy of 2 or more individuals, any one of those individuals may make a complaint ..."**

16.60 **Procedure for hearing data subject complaints** As circumstances will vary so much between complaints, it is essential that the Privacy Commissioner has a discretion in the manner he conducts investigations, subject only to the requirements of fairness. The statutory procedures should have built into them adequate standards of procedural fairness. Failure to so provide may invite litigation on whether, as a matter of interpretation, the statutory procedures should be supplemented by the common law rules of procedural fairness known as "the rules of natural justice." The Commissioner for Administrative Complaints Ordinance (Cap 397) includes the usual legal formulation, also widely adopted by data protection acts, conferring a procedural discretion, subject to certain safeguards regarding fairness. The respondent must be informed at the outset that a complaint against him has been received. Section 12(3) of the ordinance provides that the Commissioner may hear or obtain information from such persons, and make such inquiries, as he thinks fit ... and may regulate his procedure in such manner as he thinks fit." To avoid uncertainty and afford additional flexibility, it adds that "it shall not be necessary for the Commissioner to hold any hearing and ... no person shall be entitled to be heard by the Commissioner." This is subject to an express right for a person to be heard if the Commissioner is proposing to make an adverse report or recommendation on him. A similar procedural structure is found in several data protection acts, such as the Australian Act. By comparison, the UK Act is silent on procedural matters. We prefer the more explicit approach and **we recommend adoption, suitably adapted, of the procedural provisions of Cap 397.**

16.61 If these recommendations are adopted, the Privacy Commissioner will share the flexibility his overseas counterparts enjoy in adopting as informal an approach as circumstances allow. Some complaints may be resolved by a phone call, whereas others will require the taking of statements. It would also be open to the Commissioner to conduct a hearing. Overseas data protection officials have warned, however, that a danger arising from the conduct of hearings is of the formalisation of proceedings. The conduct of hearings would also tend to militate against the emphasis on

informality and conciliation which we consider important. We accordingly expect hearings to be comparatively rare.

16.62 **Public hearings** While, in accordance with general practice, hearings should be held in public, there may be circumstances in which either the data subject or the data holder may wish the hearing to be held in private. The interests of the data subject and the data holder can be distinguished in this regard. **We have concluded that hearings should be in public but that the data subject should have the right to demand a private hearing.** To provide otherwise would mean that the prospect of a public hearing could act as a real disincentive to the lodging of a complaint. Our recommendation differs from that in the Consultative Document in that we no longer propose that the data holder have the right to demand a hearing in private. We have amended our original recommendation in this way because we consider that it is the data subject whose interests should be considered in this regard.

16.63 **Legal representation We recommend that, should a hearing be convened, the position should be similar to that under section 12(4) of Cap 397, namely that "counsel and solicitors shall not have any right of audience before the Commissioner, but may appear before him if he thinks fit." The discretion should explicitly extend to lay representation.**

16.64 **Disposal of complaints We recommend the adoption of a requirement that the Privacy Commissioner inform both parties in writing of the result of the investigation. Should he exercise his discretion and decline to conduct an investigation, or to take enforcement action following investigation, he should advise the complainant in writing of his decision or opinion and his reasons, as under Cap 397.** This duty to give reasons will expand the reach of judicial review, particularly where error on the face of the record is asserted.

16.65 Should the Commissioner decline to investigate or take enforcement action, the complainant may wish to have the matter judicially reviewed. We note that in his 1989 review the UK Registrar goes further and recommends that when the authority declines to take enforcement action, data subjects should be entitled to seek an order to take action from the specialist data protection tribunal. The Home Office review disagrees with this, arguing that enforcement on most matters should be left to the Registrar because the principles can be difficult to interpret and he should not be pre-empted from proceeding by way of negotiation and warning wherever possible. **We recommend that data subjects may judicially review (but should not have the right to have reviewed on its merits) a decision of the Privacy Commissioner not to investigate a complaint or not to take enforcement action following an investigation.** We think that judicial review provides an adequate oversight mechanism in this regard. In addition, the UK experience indicates that it is unlikely to be a problem in practice, as a complainant's lack of merit will seldom be evident without the Privacy Commissioner's making initial inquiries.

16.66 **Investigations without complaints** Data protection laws differ in their definition of the enforcement agency's powers to investigate complaints. The UK Act, for example, does not explicitly authorise the Registrar to investigate matters at his own initiative. As he comments in his 1989 review, "the Registrar has no express investigation powers. Investigations are carried out because they are essential if proper consideration is to be given to those complaints which the Registrar has a duty to consider."[7] Only data subjects can lodge complaints. However, other provisions of the UK Act envisage the Registrar adopting a more proactive role, such as powers to refuse data uses through his registration role and to issue enforcement notices if satisfied that there has been a contravention of the data protection principles. As a result, the Home Office review is able to conclude that, apart from the right of data subjects to sue for compensation, "enforcement is achieved through the Registrar acting on his own initiative or after receiving a complaint." Other jurisdictions such as Canada and Australia are more explicit in empowering the enforcement agency to initiate investigations of suspected breaches of the principles. Such investigations may, like the investigation of data subject complaints, be simple affairs requiring little more than a phone call. They therefore differ from the comprehensive on-site inspections discussed below. Of course, if the Privacy Commissioner wishes to initiate a comprehensive investigation to dispel his suspicions of non-compliance, it may be appropriate for him to conduct a thorough on-site inspection. **We recommend that the Privacy Commissioner be expressly empowered to conduct investigations in the absence of a complaint, provided he has reasonable grounds for suspecting a breach of the data protection law.**

16.67 **Remedies for substantiated complaints** One of the major distinctions between data protection laws is the extent to which they confer mandatory enforcement powers on the Privacy Commissioner. Some authorities rely on an "advisory" or "persuasive" approach, with the ultimate sanctions of appealing to the legislature or the media. This is the approach adopted by the Federal Canadian legislation, for example. The Commissioner for Administrative Complaints is a local example. It will be noted, however, that both these examples relate to agencies exclusively overseeing the public sector. We are firmly of the opinion that such an approach is inadequate as regards regulation of the Hong Kong private sector. The UK legislature came to the same conclusion, so that the UK Data Protection Act virtually bristles with mandatory enforcement powers. To provide the necessary checks and balances, however, we think it should be for the courts to give the Privacy Commissioner's directives mandatory force. Accordingly **we recommend that upon finding a complaint substantiated the Privacy Commissioner should be empowered to direct the remedy of the breach in a specified manner. The data user's Responsible Officer should be subject to a duty to notify the Commissioner that compliance has been effected. Failing compliance, the Commissioner should seek an enforcement order in court. We further recommend that, as an ultimate sanction, the Privacy Commissioner may seek an order prohibiting an organisation**

[7] Fifth Report of the Data Protection Registrar, June 1989, London: HMSO, para 199.

from processing personal data. This latter power is also provided for in section 11 of the UK Act, and is only to be exercised if compliance with the data protection principles cannot be adequately secured by an enforcement order. As with an enforcement order, we recommend that the Privacy Commissioner must satisfy a court that such a prohibition order is warranted.

16.68 **Compensation for complainants** The final aspect relating to complaints requiring consideration is compensation. Article 23 of the draft Directive provides:

> *"Member States shall provide that any person whose personal data are undergoing processing and who suffers damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered."*

16.69 Compensation provides financial redress for loss or damage. The UK Home Office has described its two main purposes as being to provide a form of relief for the individual and to serve as a sanction encouraging good practice. Data protection legislation commonly provides for the payment of compensation, but the scope of such provisions vary. Some data protection legislation (the Australian Act is an example) provides that compensation may accrue from any breach of the principles. The UK Act is considerably more restrictive, limiting compensation claims to those involving damage and distress arising from data inaccuracy, or unauthorised disclosure. The UK Registrar has recommended that this be changed and that the Registrar be empowered to direct compensation up to £5,000 for damage and associated distress arising from any breach of the principles.[8] The Home Office review counters that under such a proposal:

> *"... the Registrar would be pressured by data subjects into using formal action when informal action would have sufficed; his contacts with data users would become more confrontational; and even under a consent system there may be pressure to give undue emphasis to detailed consideration of the circumstances of a small proportion of data subjects at the expense of the important task of ensuring general compliance with the principles "*[9]

16.70 These are relevant considerations, although the Home Office concedes that they involve an element of speculation, since no compensation claims had been lodged by that time. Interestingly, compensation claims appear to be uncommon. We were informed by Carol Wallace of the Quebec data protection authority that of the 250 or so complaints she had investigated over four years, she could not recall any involving a significant compensation claim. More fundamentally, however, we can see no basis in principle for

---

8 Fifth Report of the Data Protection Registrar, June 1989, London: HMSO, para 214.

9 Home Office, *Review of the Data Protection Act" Report on Structure,* HMSO, 1990.

singling out some breaches of the principles as compensatable and barring others across the board. We note that the draft Directive provision is of general application. **We accordingly recommend that a right to compensation should accrue from any breach of the data protection principles causing loss or injured feelings. (Chapter 8 recommends that inaccurate data should not be compensatable during the transition period. Chapter 12 recommends that inaccurate data not be compensatable if the data recorded is an accurate copy of the data received and identified as a copy of such data.)** In accordance with general principles, the onus will rest on the party making the assertion, namely the claimant. We recognise that compensation for injured feelings is not commonly provided for, but there is a statutory precedent in fatal accidents legislation which includes payments as solace for a death. It also accords with the approach taken by Lord Keith to the analogous issue of what constitutes "detriment" for the purposes of breach of confidence. He noted that harm to the confider may be intangible, such as injured feelings[10]. It will, in any event, be for the court to determine quantum.

16.71 The Coalition of Service Industries and several other respondents expressed concern to us that a right to compensation for injured feelings might be subject to abuse. We doubt that in practice there would be a problem. We believe that the court can be relied on to provide protection against such abuse. Claimants would be deterred from pursuing spurious claims by the prospect of having to pay costs.

16.72 **Appropriate body to determine compensation** The question remains as to who should determine compensation claims. The Privacy Commissioner will possess the expertise to determine the potentially difficult issue of whether there has been a breach of the principles causing loss. Further, his involvement in the investigation of complaints will equip him to make such a determination. Remitting the issue afresh to another body would entail duplication of effort. We agree with the Home Office's comment, however, that the power of a data protection authority to award compensation "would vest in a single authority an undesirable combination of enforcement and punitive functions." **We accordingly recommend that the Privacy Commissioner's role be limited to determining whether there has been a breach of the principles. Upon his so certifying, it would be for a court to determine the appropriate amount of compensation payable, if any. The status of the certificate in the court proceedings will be that of *prima facie* evidence, rebuttable on the balance of probabilities**. We would expect such an arrangement to encourage the settlement of claims out of court. Additionally, as claims are likely to be for comparatively small amounts, they will often fall within the jurisdiction of the Small Claims Tribunal.

[10] *AG v. Guardian Newspapers Ltd (No. 2)* 3 All ER 545, at 639.

On-site inspections

16.73 These are referred to in other countries as data protection "audits" but, as that term might appear overly negative, we prefer "verifications". However described, we consider them a vital function for an effective data protection body. The Australian Act provides the Privacy Commissioner with the power to conduct audits of personal records and has referred to this in his 1991 Annual Report as the "key method" of monitoring compliance. Similarly, in his comprehensive review of the operation of data protection authorities, Flaherty concludes that together with the investigation of complaints, agency-initiated inspections of personal information systems are the most important function of a data protection agency. His description of the exercise of this function by the German agency usefully summarises its practical operation[11]. Inspection teams are particularly concerned with such matters as illegal processing, security weaknesses, and retention of obsolete data. To facilitate an assessment of the data flow of the system being studied, prior to the site visit's being conducted, the inspection team studies the relevant organisation charts, laws and regulations. Personal data flows are traced with the assistance of charts. Upon visiting the site, the inspection members may meet the organisation head and other relevant employees such as the data protection officer and on-line operators. Inspection members usually have a background in data processing, rather than law, to equip them to ask technical questions, such as what defence strategies are taken against intrusive measures.

16.74 This account (summarised from Flaherty) was usefully supplemented by our discussions with the Federal German data protection authority. We were informed that although inspection teams attended sites for between 1 and 2 weeks, no disruption had been caused, or claimed to have been caused, to the activities of inspected organisations. The banking sector had initially expressed concern that inspections could endanger the confidentiality of their customer records, but this is no longer argued. The agency would provide advance notice of the inspection and this alone could usefully precipitate the introduction of improved procedures prior to the visit.

16.75 We note that the UK law does not at present provide the power to initiate systematic inspections. In his 1989 review of the Act's operation, the Registrar asked consultees whether he should have such a power. He reports that "perhaps not surprisingly, the majority of respondents rejected the suggestion on the ground that it would be an unnecessary intrusion into the affairs of data users when there was no significant evidence of regular data abuse."[12] A similar sentiment was expressed by the Home Office Review. In view of the German experience cited above, we disagree. The UK Registrar recommends that such a power be added, notwithstanding the negative consultation response.

16.76 **We accordingly recommend that the Privacy Commissioner have the power to initiate systematic inspections of personal data**

---

11 Flaherty, *op cit*, page 343.

12 Fifth Report of the Data Protection Registrar, June 1989, London: HMSO, para 206.

systems. This would enable him to confirm that the data protection principles are being complied with and that appropriate control systems are in place. This would entail verifying the accuracy of the organisation's description of data purposes, classes of data subjects etc., in its declaration. It would go further than this, however, and involve an examination of the operational adequacy of such aspects as storage security. The Privacy Commissioner would base his selection of organisations to visit on policy and strategic considerations, but an element of chance may also play a part in selection. We expect that the resultant difficulty for data users in predicting whether they will be visited should provide them with a useful incentive to conduct their data processing properly.

16.77 We recognise that this power of inspection is a new departure for Hong Kong and could occasion concern about its potential impact on data processing operations. The German experience is encouraging in this respect, but to provide further reassurance to Hong Kong data users, **we recommend that it be expressly provided that the power be exercised in a manner that does not unduly disrupt the organisation's daily operations.** As some respondents have expressed disquiet about the powers of the Privacy Commissioner, we also think it desirable that the private sector be utilised in conducting these inspections instead of relying exclusively on the Privacy Commissioner's staff. Australia utilises accounting firms and we recognise that Hong Kong possesses several professional organisations that would be well suited in this regard. Security clearances may be appropriate for some inspections. We think it important that the exercise of the Privacy Commissioner's power to carry out on-site inspections should be subject to some system of checks and balances. The Commissioner's selection of organisations for systematic on-site inspections will be based on policy and strategic considerations and we think the Board could usefully play a role in this situation. **We therefore recommend that the Privacy Commission provide for the board's approval a schedule of organisations for inspection.** We do not think that this monitoring role should extend, however, to the Privacy Commissioner's investigation of data users without a complaint. We have recommended that this power only arise when the Privacy Commissioner reasonably suspects a breach of the principles. A part-time board is not a suitable body to review such operational assessments.

16.78 **Inspections and secrecy** A related concern of organisations may be the confidentiality of data. Again, the German experience is encouraging, but to provide specific protection **we recommend that enforcement authority personnel be subject to a legal duty of secrecy subject to criminal sanctions.** This would put inspection and other staff on the same footing as other officials dealing with confidential information, such as those employed by the Inland Revenue Department (see Chapter 3). The obligation of secrecy would extend beyond inspections and encompass all information acquired in the course of duties, be it personal data or trade secrets.

Administration of declaration system

16.79 **Declarations and the data protection principles** We have recommended as a fundamental feature of an enforcement scheme the requirement that data users furnish the Privacy Commissioner with a declaration briefly describing their record systems. The declaration of public sector organisations would briefly describe record purposes, contents of records, classes of data subjects, classes of transferees, jurisdictions to which data export was proposed, and contact details of the organisation's Responsible Officer. Private sector declarations must only specify the first and last items but the Privacy Commissioner may consider more detailed coverage desirable. This recommendation was made in the context of ensuring that personal data are held in accordance with the Purpose Specification Principle. We further recommended that a copy be furnished to a central authority to enable data subjects to ascertain the existence of data relating to them. This was to increase transparency, as required by the Openness Principle. Making declarations public documents would assist in this regard. To this end, we recommended a system providing interested individuals with on-line access to the contents of declarations.

16.80 **Declarations and the functions of the agency** In addition to facilitating the implementation of the data protection principles, commentators attribute several other benefits to a declaration system. The compilation of a declaration requires data users to think through their record-keeping arrangements, and may also foster a sense of commitment. The system will also facilitate the regulatory oversight authority's performance of its other duties, provided there is a standard requirement that the authority be furnished with a copy. This requirement (which we recommend above) enables the agency to monitor data uses. It also provides the authority with a list of data users. The authority should accordingly be better placed to make well informed decisions regarding deployment of resources for investigations and on-site inspections. Indeed, declarations will furnish the agency with an essential starting point in the conduct of such inspections. Policy formulation should also benefit.

16.81 **Avoidance of bureaucracy** We accept that a system requiring the Privacy Commissioner to be furnished with declarations has the benefits outlined above. Our concern has been that the administration of the system does not sap the Commissioner's limited resources, nor constitute an administrative burden on data users. We are acutely conscious of the experience of other jurisdictions in this regard. They are graphically described in Flaherty's recent comprehensive review. He singles out the French and Swedish systems as deflecting enforcement in other areas, through the excessive burden of their registration requirements. Those two jurisdictions require not only that data users furnish the authority with a declaration, but also that the authority has a duty to decide whether to accept or reject the proposed data uses. This is also the UK position.

16.82 It is not surprising that an approval requirement regarding declarations is likely to engage much of an enforcement agency's resources.

We do not foresee similar difficulties with a pure notification system. The problem is that if data users are aware that the Privacy Commissioner is legally obliged to accept any notification, no matter how obviously defective, it could encourage abuse. **We accordingly recommend that the Privacy Commissioner should not be required to approve data uses described in declarations. The extent of his legal duty in responding to declarations should be to store them in a publicly accessible form. He should be empowered, however, to require further and better particulars when he sees fit.** It follows that we only envisage the Commissioner scrutinising declarations on a random basis, but the recommended power would help to ensure that data users compiled their declarations with care.

Prosecutions

16.83 The Consultative Document did not address the issue of criminal sanctions. Several respondents sought clarification. We think that the United Kingdom provisions provide a suitable model. They differentiate between those offences involving an element of knowledge or recklessness, and those lacking these elements. The former are indictable and the latter summary offences. The UK Data Protection Act provides that the following constitute criminal offences:

(i) unregistered holding of personal data;

(ii) processing of data contrary to registration details;

(iii) non-compliance with an enforcement notice;

(iv) contravention of a transfer prohibition notice;

(v) unauthorised disclosure by a computer bureau;

(vi) furnishing false information in connection with an application for registration, or failing to keep an up-to-date registered address; and

(vii) obstruction or failure to render assistance concerning search warrants.

Those at (vi) and (vii) can only be tried by summary proceedings. The remaining offences are triable either way. Regarding the appropriate level of penalties, **we recommend that summary offences should face a maximum fine of $50,000, whereas indictable offences should face an unlimited fine as well as destruction or amendment of the offending data.**

Education and publicity

16.84 Perhaps the single greatest obstacle to the implementation of data protection measures is lack of knowledge by the ordinary data user. The importance of this element is highlighted by the UK Data Protection Registrar's annual reports. In his report for the period ending June 1992 he refers to the "massive awareness task to be carried out, both for individuals and for data users." His activities included an advertising campaign, distribution of materials (introductory leaflets, newsletters, and guidance notes), production of a video, one-day seminars, 15 shows throughout the country, 24 news releases, 16 radio interviews, 7 television appearances, 54 talks, and Enquiry Service responses to 39,261 telephone calls and 13,338 letters. The latest report to hand of the Australian Privacy Commissioner describes a similarly varied range of activities. This highlights the point that comprehensive annual reports themselves perform an important publicity role. **We accordingly recommend that the Privacy Commissioner be required to compile an annual report to the Governor which should also be laid before the Legislative Council.**

Powers of the Privacy Commissioner

16.85 We have recommended above a number of functions for the Privacy Commissioner. The effective discharge of several of these, namely the investigation of complaints and inspections, requires that the Commissioner possess adequate legal powers to obtain evidence and enter premises. In formulating our recommendations we have been concerned to avoid a heavy handed approach in providing legal powers in this new sphere of regulation. We have accordingly favoured availing the Privacy Commissioner of established legal remedies, albeit with some modifications, rather than coercive new powers which bypass both data user consent and the courts.

Entry to premises

16.86 Investigations, whether in response to a complaint or on the initiative of the authority, will sometimes necessitate entry to premises. The other major function of the Privacy Commissioner, namely verification inspections, will necessarily entail such visits. In the absence of legal authorization, entry will be illegal without the consent of the occupier. We expect that such consent will normally be forthcoming, but that legal back-up procedures should be available in case it is not. **We accordingly recommend that in those cases which the Privacy Commissioner does not consider urgent, he should initially approach the organisation's Responsible Officer. If consent is not forthcoming at that stage, the Commissioner should serve a notice advising that if consent is not received within 14 days then he would seek a court order and costs.**

Urgent cases

16.87 This comparatively protracted procedure is obviously inappropriate for urgent cases, such as where large-scale transborder data exports are feared imminent. **We recommend that where urgent entry is necessary, the Commissioner should approach the court forthwith, thereby dispensing with the 14 day grace period. In such cases, the Commissioner will consider it inadvisable to alert the organisation to his imminent visit. He may, for example, fear the destruction of evidence. In these circumstances, we recommend that he be empowered to approach the court direct for an order along the fines of an *Anton Piller* order authorising entry and seizure.** The name of the order derives from the English Court of Appeal decision of *Anton Piller KG v. Manufacturing Process & Ors*[13]*.* That decision upheld the validity of the procedure whereby the plaintiff may apply for a court order against an absent party. Commonly used in copyright proceedings, this procedure would be invoked when alerting the other party to the proceedings is likely to result in the disappearance of the infringing materials.

16.88 We note the concern of the Bar Association that an order akin to an *Anton Piller* order should be used sparingly. We are conscious that such an order should be with care and only in unusual circumstances. We would not expect the Commissioner to need to resort to this procedure in more than a handful of cases and we are satisfied that the scrutiny of the court will ensure the power is not abused. The position of the Commissioner means that he is likely to adopt a more objective approach to the use of this power than would be the case where a private citizen sought an *Anton Piller* order.

Evidence

16.89 The Privacy Commissioner will need to gather evidence when investigating suspected contraventions of the legislation. This may consist of his own observations, in which case there is no problem. This may need to be supplemented, however, by answers to questions and the seizure of material. The lack of a power to compile evidence can inhibit the effectiveness of a data protection authority. The UK Act at present lacks express powers requiring data users to respond to questions. In his 1989 review, the UK Registrar reported that his investigators had found that individuals working for organisations were often hesitant about furnishing evidence in the absence of a duty to do so. He accordingly recommended that he be empowered to serve notice on any person to furnish in writing such information (as specified in the notice) as is necessary or expedient for the performance by the Registrar of his functions. Such a notice would be appealable. The Home Office Review endorses this recommendation, except that only data users should be subject to such notices in the absence of a court order. Such a power is already provided for in other data protection laws, such as those of Australia (section 44), Germany (section 24) and the

[13] [1976] 1 All ER 799.

Netherlands (section 45). In Hong Kong, Cap 397 confers substantial powers on the Commissioner of Administrative Complaints in this regard. These encompass a requirement to furnish the Commissioner with any information (on oath if the Commissioner thinks fit), and to produce any document or thing. This legislation also carefully addresses such ancillary matters as over-riding secrecy provisions, limiting the use of answers in other proceedings, and restrictions where it is certified that public interests such as national security may be prejudiced. **We recommend a power to require persons to furnish information along the lines of Cap 397, subject to our recommendation below regarding the taking of evidence on oath.**

Exempt data

16.90 The UK Registrar has identified a potential problem that is best avoided. Under the UK Act, the powers of inspection and seizure are not applicable to data which are subject to one of the exemptions discussed in chapter 15. The difficulty is that it is first necessary to examine the data to ascertain whether they are subject to an exemption. The Home Office review agrees that there is a problem and recommends that the Registrar be empowered to seize any material, provided that he has reasonable cause to suspect that the Act has been contravened in respect of some of its contents and that any exempt data are returned within a reasonable period. **We recommend a provision to similar effect**.

Appropriateness of oath requirement

16.91 We considered whether a power to obtain information on oath is necessary. Such a power is widely provided for in Hong Kong legislation, but is seldom invoked. Our concern is that the formality implied by this power may convey to the public that the agency is another wing of a powerful and perhaps authoritarian administration. This would be at variance with our aim of constituting an enforcement body which is not perceived as remote and forbidding, but rather one possessing only the minimum powers necessary when an informal approach fails. For these reasons, **we recommend that the Privacy Commissioner should not be empowered to obtain evidence on oath, but that instead it should be a criminal offence to wilfully make a false statement to the Commissioner.**

Review and Appeal Procedures

16.92 In keeping with our concern to establish a system of checks and balances, **we consider adequate appeal powers an important aspect of a data protection regime. Like other officials, the Privacy Commissioner's decisions should be subject to judicial review and we so recommend.** Judicial review is a limited remedy, however, as it does not entail a reconsideration of the merits of the decision. While we favour the right to appeal on the merits from decisions made by a public authority vested with

powers similar to those we have recommended for the Privacy Commissioner, we do not consider a court the ideal body to consider the comparatively specialised issues involved in an appeal on the merits (as opposed to an appeal on a question of law) on data protection issues. The UK solution has been to constitute a specialist tribunal to consider appeals from the Registrar's decisions. We agree with this approach. **We therefore recommend that appeals by data users and data subjects be considered by the Administrative appeals Board.** The Board should establish a panel of potential members with expertise relevant to the consideration of data protection matters. The Board would be constituted from members of this specialist panel when hearing a matter to which the Privacy Commissioner is a party.

16.93 Our recommendation on this differs from that in the Consultative Document, which proposed a separate specialist tribunal. On further consideration, we believe that this would be unnecessarily costly, and would be serve no particular purpose in view of the already established Administrative Appeals Board which we are confident can satisfactorily fill the role.

Chapter 17

Transborder data flow

Summary

17.1 This chapter examines the controls which should be imposed on the transfer of personal data to jurisdictions lacking adequate data protection, whether or not the transfer is by automated means. It raises the question of the territorial scope of a data protection law in Hong Kong. We conclude that Hong Kong's data protection law should apply to any personal data which is processed or controlled in Hong Kong, regardless of whether or not the personal data is held within the territory.

17.2 If the general provisions of the law accordingly apply to personal data which has been transferred to another jurisdiction but is processed or controlled here, no additional provisions are required dealing specifically with transfer. Should the transfer of data be accompanied by a loss of control of its use, however, we believe that specific measures may be required.

17.3 We do not think that transfers of data outside the jurisdiction either for public purposes or for purposes which involve the consent of the data subject should be subject to additional controls, whether or not they also involve transfer of control. Those transferring data not falling within these categories should be subject to a duty to take all reasonably practicable steps to ensure that the data protection principles apply to the data while held in the other jurisdiction. This duty can be discharged in various ways, including the application of a data protection law in the other jurisdiction, sectoral codes of practice, or contracts. Failure adequately to discharge the duty will expose the data transferor to intervention by the Hong Kong data protection authority.

Recommendations

17.4 The general provisions of the data protection law should apply to the processing of personal data in Hong Kong, whether or not the data controller is in the territory. Equally, data processing outside Hong Kong which is controlled from within the territory should also be subject to the general application of the law (paragraph 17.18).

17.5 The transfer of data out of Hong Kong should be legally regulated, regardless of the medium by which it is transferred. It should also extend to a telecommunications link not necessarily entailing its being recorded by the international recipient. (paragraph 17.21)

17.6 A data transfer to another jurisdiction which does not ensure an adequate level of protection may take place on condition that:

(i) the data subject has consented to the proposed transfer in order to take steps preliminary to entering into a contract;

(ii) the transfer is necessary for the performance of a contract between the data subject and the controller, on condition that the data subject has been informed of the fact that it is or might be proposed to transfer the data to a country which does not ensure an adequate level of protection;

(iii) the transfer is necessary on important public interest grounds of the kind discussed in Chapter 15; or

(iv) the transfer is necessary in order to protect the vital interests of the data subject (paragraphs 17.22-23).

17.7 As regards other cases, a specific legal obligation should be imposed on Hong Kong data users transferring data without retaining full control over their use in the other jurisdiction. The content of this duty would be that data users should take all reasonably practicable steps to ensure that the transferee complies with the data protection principles as regards the transferred data. The duty is distinct, however, from the duty of care contained in the legal action of negligence, as it would not be directly enforceable by data subjects in the courts. Instead, as with the breach of the data protection principles, a breach would constitute the basis of a complaint to be investigated by the Privacy Commissioner. He would also be able to investigate possible breaches at his own initiative. (paragraph 17.27)

17.8 The Privacy Commissioner should be empowered to apply for an injunction when he has reasonable grounds for suspecting that a proposed transfer would result in a breach of the data protection principles. Relevant considerations would include the adequacy of data protection in the jurisdiction to which the data are transferred and the nature of the data. (paragraph 17.26)

Background

17.9 International data traffic necessarily entails transfers between countries with disparate legal systems. In her recent comprehensive review of the issue, Adriana Nugter notes that "the extended possibilities to transmit information almost without reference to distance, time or volume has given rise to a spectacular growth in data flow through the use of the international telecommunication networks."[1] The extent of this transborder data flow ("TBDF") is underlined by a 1983 study showing that 85% of companies surveyed depended on TBDF for at least one key aspect of their international operations.[2] Nugter aptly characterises this traffic as "the life-blood of modern business life." The dilemma arising from this ever increasing flow of personal

[1] Adriana Nugter, *Transborder Flow within the EEC*, (Computer Law Series: Kluwer, 1990), page 204.

[2] Nugter, *ibid,* page 204.

data between countries derives from their greatly variable levels of privacy protection. Adoption of our recommendations will provide a good level of personal data protection within Hong Kong. This will decrease the territory's vulnerability to transborder prohibitions by other jurisdictions. As emphasised in Chapter 2, this is a major reason why Hong Kong should enact comprehensive legislation as soon as possible. We have recommended that this legislation be based on the OECD data protection principles. It is relevant to recall in this context that the impetus for the formulation of these principles was the need to rationalise the international regulation of data flows through the harmonisation of national laws. By joining a number of other jurisdictions that have adapted or enacted laws to secure harmony with these principles (including within the region Japan, New Zealand and Australia), Hong Kong will be well placed to benefit from uninterrupted data traffic from its trading partners.

The need for transborder controls

17.10 Even jurisdictions possessing data protection laws often lack provisions controlling the transfer of data out of the jurisdiction. Increasingly, however, the climate of international concern over "data havens" (jurisdictions without adequate privacy protection regulating data processing) is finding legal expression in domestic legislation. The whole issue has been highlighted by the draft Directive, a stated aim of which is to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner. The draft Directive recognises that data will also be exported outside the community to third countries with differing degrees of data protection. Article 26(1) states the basic position:

> *"The Member States shall provide that the transfer, whether temporary or permanent, to a third country of personal data which are undergoing processing or which have been collected with a view to processing may take place only if the country in question ensures an adequate level of protection."*

17.11 The remaining clauses of the article allow data to be transferred to a country lacking an adequate data protection law in certain circumstances examined below. We conclude that the legal regulation of TBDF is an important feature of comprehensive data protection legislation. **We recommend that the transfer of data out of Hong Kong be legally regulated, but in a manner that avoids bureaucratic controls. Our detailed proposals are spelt out later in the chapter.**

Territorial scope of data protection laws

17.12 The simplest logical method of regulating data transferred from the territory would be to subject it to the same regulatory framework as that applied within Hong Kong, whether or not the data processing was conducted

or controlled in Hong Kong. But giving the law this extraterritorial scope is subject to the constraints of constitutional law.[3] A common law doctrine of uncertain ambit limits the ability of a colonial legislature to enact laws with extraterritorial effect. The basis of this limitation derives from the limited grant of legislative power accorded colonies such as Hong Kong. Hong Kong is only empowered to enact legislation for the "peace, order and good government" of the colony. Laws which do not have a "real and substantial relation" to the colony are vulnerable to being struck down as invalid by the courts. Such a nexus may not be made out merely because the data processed out of Hong Kong relates to a Hong Kong resident. The Hong Kong (Legislative Powers) Order 1986 provides for some limited exceptions which would not encompass data protection. There is also the practical consideration that if the data are not processed or controlled within Hong Kong, effective enforcement action by the local oversight authority is precluded. This is no doubt why other countries not subject to this territory's constitutional limitations have legislated in terms that ensure that effective enforcement remains feasible.

17.13 A few examples will suffice to indicate some of the main approaches taken by other countries in determining the territorial scope of their data protection laws. The French law fixes legal liability on data users involved in even the partial processing of personal data (eg collection) within France. If the processing is carried out by a foreign data user's agent (eg a computer bureau), that agent must be identified in the declaration as the foreign data user's representative and as such is subject to the law. This ensures that legal redress is always available against someone present within the country.

17.14 The UK law focuses not on whether processing takes place within that country, but on whether control over such data is exercised within the UK. This may result in a broader territorial sweep to the UK law, as compared with its French counterpart, in that the UK law applies where control is exercised within the UK, even if the processing is carried out elsewhere. As regards computer bureaus, however, the determining factor is whether the processing is carried out in the UK.

17.15 A further variant is provided by the Netherlands law, whose territorial scope is primarily determined by whether the file is located within the country. Nugter points out that a consequence of this diversity of approaches to territorial application is that of potential overlap. A file located in the Netherlands and processed in France by a computer bureau at the behest of a UK based data controller will be subject to laws of all three countries. Conversely, the application of different tests may result in no law being applied.

17.16 In choosing an appropriate criteria to determine the territorial scope of a data protection law for Hong Kong, the two obvious factors are control and processing. We think it important that, in the interests of

[3] Peter Wesley-Smith, *Constitutional and Administrative Law in Hong Kong*, (Hong Kong: China & Hong Kong Law Studies Ltd), 1988 pages 273-5.5.

promoting the continued free flow of data to Hong Kong, Hong Kong not become a data haven, free of effective controls on personal data. To that end, we think it important that, for instance, the data protection law in Hong Kong should continue to apply to a data controller in the jurisdiction, even where the data has been transferred to another jurisdiction.

17.17 There are three ways of providing transborder data protection. The first would be to apply the legislation to processing controlled by a data user within the jurisdiction (as in the United Kingdom). The second would be to apply the provisions where processing of the data had taken place within the jurisdiction (as in France), and the third would be to apply the provisions if the data related to citizens of that country. The sub-committee took the view that a control test should be applied but we have concluded that this needs to be supplemented by the second test, whereby the law would apply to data processed in Hong Kong, whether or not the data controller was based here. This would reassure other countries that Hong Kong would not become a data haven. For example, the data controller based in France might only be prepared to transfer data to Hong Kong if the data continued to be subject to a data protection law. The French law would cease to protect the data following transfer, as that law lacks a control test. Nor would the control test apply to the processing of data in Hong Kong, with the data controller situated in France. The regulatory gap can only be filled by applying the Hong Kong law to data processed here.

17.18 **We accordingly recommend that the general provisions of the data protection law should apply to the processing of personal data in Hong Kong, whether or not the data controller is in the territory. Equally, data processing outside Hong Kong which is controlled from within the territory should also be subject to the general application of the law.** We note that this approach is in line with Article 4 of the draft Directive.

Imported data

17.19 Upon importation of data, the data protection principles will apply. But several direct marketing organisations have sought clarification of the status of data compiled in contravention of the principles. We think that such data must be treated as valid in the absence of a challenge from the data subject. The data subject should, however, be entitled to challenge the data whether or not he resides in Hong Kong. In Chapter 13 we therefore recommended that access and correction rights not be restricted to Hong Kong residents.

Regulation of data exports not subject to general provisions of the data protection law

17.20 In view of this emphasis on the control of data, the transfer of data does not mean that it will cease to be subject to the full application of the

Hong Kong law. If data are transferred out of Hong Kong but control is retained within Hong Kong (eg transfer to a data bureau solely for processing and return to Hong Kong for use), the data will remain subject to the general application of the Hong Kong data protection law. The specific transborder regulatory provisions described below will only need to apply in the converse situation where the transfer is accompanied by a loss of control over the data. Accordingly, all data transfers will be legally regulated, but the applicable regulatory regime will be determined by whether control over the data is retained within Hong Kong. The remainder of the chapter addresses the extent to which the transfer of data not subject to the general application of the law should nonetheless be regulated.

Definition of transfer

17.21 The international exchange of data is primarily an electronic processing phenomenon but non-automated exchanges such as posted mail or tape recordings, also commonly occur. We have earlier recommended (in Chapter 8) the regulation of personal data regardless of the storage medium. Nor do we propose differential controls in the present context. We also note that other data protection laws encompassing manually processed data (eg France, Germany, and the Netherlands) envisage a similarly broad application to the transfer of data. A similar approach apparent in the UK law, although the law is restricted to the automatic processing of data. **We accordingly recommend the regulation of the transfer of data in whatever form.** This transfer will often be in the form of fleeting electrical impulses transmitted onto the recipient's monitor screens, and to this extent transcends our particular concern with personal data records. The issue was identified by the UK Registrar in his 1989 review and he recommended that the TBDF provision in the Act be amended to put beyond doubt his power to regulate the transfer of data by a telecommunications link not necessarily entailing its being recorded by the international recipient. **We similarly recommend.** We also wish to clarify a point obscured by the Consultative Document's reference to the "export" of data. Rather, the issue is whether the data is transferred to another jurisdiction. Such a transfer may be from Hong Kong to another jurisdiction or it may be a transfer between two other jurisdictions directed from Hong Kong.

The draft Directive and permissible data exports

17.22 One of the most significant alterations to the latest (October 1992) version of the draft Directive is its significantly more flexible approach to data transfers to third countries. We have quoted above its general requirement that such transfers "may take place only if the [receiving country] ensures an adequate level of [data] protection." Article 26(2) goes on to provide that:

"Member States shall provide that a transfer to a third country which does not ensure an adequate level of protection may take place only on condition that:

> *subject, where appropriate to article 8(2)(a), the data subject has consented to the proposed transfer in order to take steps preliminary to entering into a contract;*
>
> *the transfer is necessary for the performance of a contract between the data subject and the controller, on condition that the data subject has been informed of the fact that it is or might be proposed to transfer the data to a third country which does not ensure an adequate level of protection;*
>
> *the transfer is necessary on important public interest grounds; or*
>
> *the transfer is necessary in order to protect the vital interests of the data subject.*

17.23 **We recommend adoption of this provision.** It follows that provided a data transfer comes within these grounds, it should not be subject to any additional legal restrictions (other than the application of the general provisions of the data protection law, if data processing or control is retained within Hong Kong).

Transborder data regulation in other countries

17.24 In view of the above, we can restrict our attention to legal regulation of data transfers which are neither subject to the general provisions of the data protection law (because the data are controlled from Hong Kong), nor fall within the scope of article 26(2). The Hon Justice Michael Kirby has succinctly summarised the general features of TBDF controls adopted in other jurisdictions as follows:

"In some countries, TBDF are treated by legislation as just another aspect of the transfer of personal data ... In Austria, on the other hand, in some circumstances the data user or collector must be granted a licence before any personal data is transmitted, although the circumstances in which the licence must be sought have recently been reduced in number. The law in France, Finland and Norway permits the free flow of international personal data, subject to an overriding discretionary power of the relevant authority to prohibit or regulate such activity. Advance notice of intended data flow of this kind is required to the central authority prior to the transfer occurring. By way of contrast, in Sweden and Iceland, the prior permission of the data protection authority is generally required

before any international transfer of personal is lawful, where such data would fall within the provisions of the legislation."[4]

Approval requirements

17.25 A common requirement of the provisions summarised is that the data protection agency be notified of proposed transfers and specific consent may be additionally required. Given the ease of such transfers in an age where they can be effected by attaching modems to telephones, we are sceptical of the realism of such requirements for every transfer. If indeed data users did comply with such requirements, the very scale of the traffic could overwhelm an oversight authority without considerable resources. In this respect we prefer the UK approach. The Data Protection Act envisages an oversight role by the Registrar as regards TBDF, backed up by a power to prohibit transfers. Upon registering, a data user is required to identify in the declaration "the names or a description of any countries or territories outside the United Kingdom to which he intends or may wish directly or indirectly to transfer the data" (section 4(3)(e)). If it accordingly "appears" to the Registrar that an export is proposed, he may issue a transfer prohibition if the transfer is likely to lead to a contravention of the data protection principles. To date, the registrar has issued one such notice. In 1990 he issued a notice prohibiting the transfer of names and addresses to the USA for the purposes of direct mail. In the circumstances the Registrar was satisfied that the transfer would be likely to lead to a contravention of the data protection principles.

Power of intervention to prevent data transfers out of Hong Kong

17.26 We agree that the Privacy Commissioner should be able to intervene in circumstances such as these. We also agree that declarations could play a pivotal role through a requirement that data users identify all jurisdictions to whom they propose transferring data, and specifying whether control will be retained within Hong Kong over that data. As a mechanism of intervention, however, we would prefer that the Commissioner be required to take out an injunction in the courts, rather than a prohibition notice along UK lines. Admittedly there is little in it, as the UK law provides that a transfer prohibition notice shall not take effect until the expiration of the period during which an appeal may be brought. The appropriate legal test to sustain the Privacy Commissioner's application should be whether he has reasonable grounds for suspecting that a proposed transfer would result in a breach of the data protection principles. Relevant considerations would include the adequacy of data protection in the other jurisdiction and the nature of the data. **We therefore recommend that the Privacy Commissioner be empowered to apply for an injunction when he suspects on reasonable grounds that the export of data will result in a breach of the data protection principles.**

---

4 (1988) *New Zealand Law Journal*, page 384.

A legal duty on data transferors

17.27 It follows that, as in the UK, the Privacy Commissioner is not restricted to a purely reactive role. We would go further than the UK law, however. **As regards data transfers not falling within the scope of article 26(2), we recommend imposing a specific legal obligation on Hong Kong data users transferring data without retaining full control over its use in the other jurisdiction. The content of this duty would be that data users should take all reasonably practicable steps to ensure that the transferee complies with the data protection principles as regards the data transferred. The duty is distinct, however, from the duty of care contained in the legal action of negligence, as it would not be directly enforceable by data subjects in the courts. Instead, as with the breach of the data protection principles, a breach would constitute the basis of a complaint to be investigated by the Privacy Commissioner. Consistently with the role we envisage for him, the Privacy Commissioner would also be able to investigate possible breaches at his own initiative. The Hong Kong Trade Development Council's submission sought clarification of this recommendation. We have interpreted this as a request that upon enactment of the law, the Privacy Commissioner should assist data users to determine the data protection status of jurisdictions to which they propose to transfer data. We agree this would be necessary. We therefore recommend that the Privacy Commissioner maintain a list of jurisdictions with adequate protection.**

Methods of satisfying duty to ensure compliance following transfer

17.28 At first blush it may appear unduly onerous to require data users to take steps to ensure that a transferee in another jurisdiction comply with the data protection principles where control over its use is no longer retained within Hong Kong, but the duty only applies to transfers not sanctioned by article 26(2). We expect that provision to cover the majority of data transfers to other jurisdictions. As regards the remainder, only reasonably practicable steps are required. We are not seeking an unconditional guarantee of such compliance. There will not be a problem if the transferee is in a jurisdiction where a data protection law applies to the relevant sector, be it public or private. This is acknowledged by the draft Directive, which restricts its attention to jurisdictions lacking "an adequate level of protection." In the absence of legislative protection, however, other mechanisms would have to be employed. The two principal methods which have been utilised overseas in this connection are contracts and voluntary codes. This chapter concludes with a brief examination of their operation.

17.29 **Voluntary codes of conduct** A number of international trading organisations have developed voluntary codes based on the data protection principles. For example, the International Air Transport Association has a vital concern in the unhindered international exchange of personal data required to effect flight bookings. It has accordingly promulgated a code of

Recommended Practice which members are expected to apply regardless of whether there is a data protection law in place.

17.30 **Contractual assurances of compliance** The other main method of securing compliance by a transferee in a jurisdiction lacking legal data protection is contractual. This is the method adopted by the French data protection authority when imposing conditions on the export of data. Fiat wished to transfer personal data from its Paris office to its Head Office in Italy, a country without a data protection law (although under our proposals TBDF regulation as opposed to application of the domestic law would only arise if control over the data was not retained by the transferor). The French authority was so advised and imposed the condition that the Italy office enter into a contract with its French counterpart undertaking to apply the data protection principles. From the data subject's point of view this does not provide complete legal protection. This is because under the common law principle known as privity of contract, only a party to a contract can sue to enforce it. We do not consider this such a problem in view of the legal powers we have recommended for the Privacy Commissioner in relation to the Hong Kong based transferor.

17.31 We should add that this contract is given by way of example only of the mechanism involved. We are not recommending that the Privacy Commissioner be notified of data transfers on a case by case by basis, other than by having proposed transferee jurisdictions identified in declarations. In the first instance it would be a matter for the Hong Kong data transferor to assess whether it was a reasonably practicable step for him to enter into such a contract to secure compliance. The Privacy Commissioner's advice could be sought on the matter, but if, for example, the data transferor decided on the contractual solution, it would be his responsibility to prepare the documentation. The onus would remain on the data user to discharge the legal duty of taking reasonably practicable steps to ensure compliance by the transferee with the principles. In the last analysis, and if it became an issue, it would be for the Privacy Commissioner (subject to appeal) to determine whether the data transferor had discharged the legal duty we propose to apply. We do not envisage that this would entail his ascertaining the fate of the specific data following its transfer. Accordingly, we do not envisage that mutual legal assistance would be required, unlike areas such as the control of international drug trafficking.

Chapter 18

The media and data protection

Introduction

18.1 The main data protection issue we did not address in the Consultative Document was the scope of an exemption to accommodate free speech rights of the media. While we had recommended qualification on the application of the data protection principles to other competing public interests, this issue we deferred. This is a complex issue requiring analysis of the extent to which "free speech" rights exercised by "the media" should be constrained by the protections afforded by the data protection principles. The relevant parameters are provided by the Bill of Rights and our overall recommendations for an exemptions scheme. Also relevant is the extent to which alternative remedies are available to individuals adversely affected by the activities of the media. The extent to which free speech is already subject to both common law and statutory restrictions is an additional consideration.

Recommendations

18.2 The exemption applicable to the media should be restricted to data solely used for journalistic purposes (paragraph 18.12).

18.3 The Collection Limitation Principle should apply to the media (paragraph 18.48).

18.4 The Data Quality Principle should apply to the media. The media should be required to take all practicable steps to disseminate a correction where inaccurate data has been published (paragraph 18.50).

18.5 There should be an exemption from the Use Limitation Principle for data the publication of which is in the public interest (paragraph 18.52).

18.6 There should be a total exemption from the principle granting access and correction rights for unpublished data held by the media solely for journalistic purposes (paragraph 18.63).

18.7 The Privacy Commissioner should be restricted to the reactive role of investigating complaints about the media. He should not be empowered to conduct investigations at his own initiative or conduct on-site inspections (paragraph 18.66).

18.8 The declaration requirement should apply to data used for journalistic purposes (paragraph 18.67).

Definition of "the media" and the scope of an exemption

18.9 C. Edwin Baker defines the "media" as:

> *"all those enterprises or organizations whose primary product finally delivered to the consumer is speech or print or picture, whether sold or given to the public. This definition would not include the whiskey company that advertises whiskey, since whiskey, not speech, is the product the company wants to deliver to the consumer".*[1]

18.10 This definition encompasses both broadcasting and the press. As the two mediums are business competitors, we have not differentiated between them, except where strictly necessary. There are difficulties, however, in determining the scope of the definition. For example, should it encompass in-house publications? We are disposed to think that it should. What is clear is that media disclosures differ from other data users in their scale: they necessarily entail "publicity". In view of the problems of precisely identifying the ambit of "the media", our recommendations focus on journalistic purposes.

18.11 The application of the other proposed exemptions is determined not by the identity of the organization using the data but the purposes for which the data are used. More specifically, exemptions are stated to apply to the extent that the use of the data are likely to prejudice a competing social interest, such as law enforcement or public safety. Article 9 of the draft Directive couples both these aspects, namely the identity of the data user and the data purpose. This provides:

> *"With a view to reconciling the right to privacy with the rules governing freedom of expression, Member States shall prescribe exemptions from this Directive in respect of the processing of personal data solely for journalistic purposes by the press, the audio-visual media and journalists."*

18.12 **We recommend adoption of this approach whereby the applicability of any exemption in this sphere should be restricted to personal data solely used for journalistic purposes.**

18.13 The Explanatory Memorandum accompanying the draft Directive elaborates on article 9 as follows:

> *"The approach adopted lays emphasis on the obligation to balance the interests involved in granting exemptions. Account may be taken for example of the availability of remedies or of a right of reply, the existence of a code of professional ethics, the*

[1] C. Edwin Baker, *Human Liberty and Freedom of Speech* (Oxford, 1989), at 234.

limits laid down by the European Convention on Human Rights, and the general principles of law."

18.14 It would appear, therefore, that the Directive envisages a tailored approach whereby the extent of an exemption is determined in the light of the existing legal and administrative framework. This may help explain why other jurisdictions have hitherto differed considerably on the issue. The Netherlands and Switzerland totally exempt the media from the application of their data protection laws. On the other hand, data protection laws are applied in their entirety to the media by Belgium, Iceland, Ireland, Luxembourg, Sweden, and the United Kingdom. Denmark, Finland, France, Norway, Austria, and Germany adopt an intermediate position.[2] Accordingly, it is necessary to examine Hong Kong's existing laws touching on the issue.

Hong Kong Laws affecting the media and privacy

The application of the Bill of Rights

18.15 In Hong Kong, the most pertinent legal parameters are contained in the Bill of Rights. This provides legal protection to both privacy and free speech, thereby distinguishing the situation from that obtaining in many of the countries just cited, including the UK. Chapter 2 examined the protection to privacy afforded by article 14. The question now addressed is the extent to which this should be qualified by article 16's protection for free speech. This provides in part:

> *"2. Everyone shall have the right to freedom of expression: this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers either orally in writing or in print, in the form of art, or through any other media of his choice.*
>
> *3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions but these shall only be such as are provided by law and are necessary:*
>
> *(a) for respect of the rights or reputations of others; or*
>
> *(b) for the protection of national security or of public order (ordre public), or of public health or morals."*

18.16 There is little jurisprudence on the interpretation of this specific provision. However, the free speech provision of the European Convention of Human Rights is in similar terms. Reference will accordingly be made to the extensive case law construing the latter provision and its relationship to the protection of privacy.

---

[2] Council of Europe, *Data Protection and the Media* (Strasbourg 1990).

Privacy vs Free Speech: striking the balance

18.17 As pointed out by the Calcutt Committe[3], the initial issue is to determine the relative weights to be accorded to individual privacy and press freedom. The Committee cited the UK Press Council Declaration of Principle adopting as the starting point the right to privacy, infringement of which is only defensible if it is "outweighed" or "overridden" by a public benefit in disclosure. The Committee then considered the alternative approach expressed by the European Court in *Sunday Times v United Kingdom*[4] stating that it was "faced not with a choice between two conflicting principles, but with a principle of freedom of expression that is subject to a number of exceptions which must be narrowly interpreted." The Committee adopted this latter approach of starting from a position that free speech is pre-eminent, but that certain exceptions protecting the individual may prove to be necessary. This approach would also appear to be required by the Bill of Rights, which has a similar structure to the European Convention. Analysis is accordingly required of the protected zones under the free expression and privacy provisions and the extent to which it is necessary to qualify the former by the latter.

Freedom that of both communicator and recipient

18.18 The free speech provision has a dual aspect which is absent from the privacy provision. It confers the right on both the communicator and the recipient. Barendt concludes that it is principally concerned with "the public's interest in receipt of information, rather than the communicator's freedom." This is a result of what in his view is:

> *"the principal value underlying the provision, namely the preservation of political freedom ... restrictions on the free flow of political information are suspect because they invade the audience's interests in having enough material before it to make informed choices and to participate in the democratic process."*[5]

The meaning of freedom of expression

18.19 In his helpful analysis Barendt summarizes the free speech principle as:

> *"that speech, even speech which causes some measure of harm to the public, is entitled to special degree of immunity from government restraint not afforded to conduct which might cause a similar amount of damage. Under this rule, for example,*

---

3 Home Office, *Report of the Committee on Privacy and Related Matters,* HMSO, 1990.
4 (1979) 2 EHRR 245.
5 Eric Barendt, *Freedom of Speech* (Clarendon, 1985), at 1.

> *speech which offends the majority of people could not legitimately be prohibited, while there would be no comparable inhibition in restraining public conduct - love-making or leaving litter in Hyde Park - which has similar offensive characteristics."*[6]

18.20 What then is the justification for this deference to free speech? There are three major theories supporting the right. John Stuart Mill argued that open discussion facilitates the ascertainment of the truth. A second theory is that free speech is an integral part of each individual's self-development and fulfilment. A third theory supports free speech on the basis that it facilitates citizens' understanding of social and political issues and thereby enables them to participate effectively in the workings of society. Barendt concludes that it is this third theory that has been the most influential in the development of 20th Century free speech law. This is confirmed by the decisions of the European Court now examined.

Freedom to speak: some more equal than others

18.21 The free expression provision of both the Bill of Rights and the European Convention refer to the exercise of the right as involving special "duties and responsibilities". In its decision in *Handyside*[7]*,* the European Court of Human Rights considered that in determining the necessity of restricting freedom of expression to accommodate a competing interest, the words quoted require a consideration of "the particular situation of the person exercising freedom of expression and the duties and responsibilities attaching to that situation". A broader or narrower view of the scope of the restrictions required will be taken accordingly. The decisions accord the highest level of protection to the discussion of political ideas by the media.

18.22 **Political speech** The European Court considers that the media has a special role which broadens the scope of its free speech as compared with other communicators. In *Barthold*[8] the role was described as that of "purveyor of information and public watchdog". The decisions use language signifying that the media has a duty to inform the public. So in *Lingens*,[9] the Court held that it was "incumbent on [the media] to impart information and ideas on political issues just as on those other areas of public interest". It added that the public had a corresponding right to receive them. The European Court recently affirmed this approach in *Spycatcher*,[10] prompting one commentator to observe that:

> *"Although the free speech provision applies to all forms of expression, press freedom now seems to constitute a special category where the necessity for a restriction must be particularly well established".*[11]

---

6 See note 5, at 24.
7 (1976) 2 EHRR 737.
8 (1985) 7 EHRR, 383.
9 (1986) 8 EHRR 407.
10 *Observer and Guardian v United Kingdom* (1992) 92 13 HRLJ 7.
11 Peter Duffy, "Spycatcher in Europe", New Law Journal, October 13 1991, page 1704.

18.23 **Commercial speech** This was considered by the European Commission of Human Rights in X *and Church of Scientology v Sweden*.[12] The decision has been analyzed in the following terms by Van Dijk & Hoof:

> *"The Commission adopted the view that commercial 'speech' as such is not outside the protection conferred by [European Convention], but that the level of protection must be less than that accorded to the expression of 'political' ideas, in the broadest sense, with which the values underpinning the concept of freedom of expression in the Convention are mainly concerned ... [and] the test of 'necessity' should be a less strict one when applied to restraints imposed on commercial 'ideas'."*[13]

18.24 In view of these authorities we accept that the mass media deserves special protection of its role as the voice of the community. Such protection is primarily for the benefit of the community rather than the media organizations themselves. The media plays a vital role in assisting individuals to exercise their rights as citizens. A related point is that free speech plays a pivotal role in the upholding of human rights generally:

> *"A free press and other information media are, like an independent judiciary, instruments for realisation of other rights and freedoms because in a country where there is freedom of information and the information media are free, the chances are better that other rights and freedoms will also be respected. Whatever lawyers may say, the ultimate sanction of human rights is the force of an educated public opinion and it is the press and other media which both inform and educate public opinion."*[14]

18.25 Privacy is also a protected right under the Bill of Rights. As such, free speech must be qualified to the necessary extent. The European Commission of Human Rights examined the relationship between free speech and privacy in *Winer*[15]. Anthony Lester Q.C. provides the following analysis:

> *"The Winer case concerned a complaint that English law did not provide an adequate remedy, including a right of reply, for gross invasions of the applicant's privacy arising from statements published in a book which were not alleged to be either defamatory or untrue. The Commission held the complaint to be inadmissible ... The case suggests that the Commission does not wish personal privacy to be respected at the expense of free*

---

12 Application N, 7805/77.

13 P. Van Dijk & G van Hoof, *Theory and Practice of the European Convention on Human Rights* (second ed) Kluwer 1989.

14 John P Humphrey, “Political and Related Rights" in Meron (ed) *Human Rights in International Law* (Oxford, 1985), at 182.

15 Application No. 10871, Admissibility decision 10 July 1986.

speech except in gross instances of unwarranted invasions of one's private life".[16]

Common Law protections against the public disclosure of private information

18.26 Before analysing the extent to which the scope of the various data protection principles can be reconciled with the Bill of Rights free speech provision, it is also relevant to examine the availability of alternative remedies. These remedies necessarily possess another aspect that is relevant, namely that of inhibiting free speech.

Defamation

18.27 The law of defamation provides a remedy for a false statement impairing the plaintiff's reputation. It has been suggested that the difference between a right to freedom from defamation and a right to privacy is that the former is primarily concerned with one's reputation, whereas the latter "directly concerns one's own peace of mind". But as Professor Wacks points out, "this is not a distinction that has ever been a sharp one"[17] and the defamation remedy partially overlaps the protection afforded by a data protection law for the use of inaccurate information causing loss or emotional suffering. In one respect it is narrower than the data protection remedy, as the latter does not require proof of damage to reputation. In another it is wider, as it is no defence that the assertion is simply a repetition of an inaccurate statement. It will be recalled that under our data protection proposals there is liability for compensation for the transferor but not the transferee when the inaccurate data is a copy of data received from another and identified as such.

18.28 Turning from the defamation action as an aid to data protection to its potential to inhibit the media, it has been criticised as posing a "chilling" effect on free speech. It exposes a publisher to liability if in good faith he publishes allegations about a public figure which he cannot substantiate. In interpreting their First Amendment, US courts have struck the balance differently. Their Supreme Court has accordingly held that a public official suing for allegations relating to his official conduct has the burden of proving that the allegations were knowingly false.

18.29 While defamation may therefore act as a fetter on free speech, its potential to do so is reduced by the defences of absolute and qualified privilege, together with that of fair comment. This is particularly so at the crucial pre-publication stage. In deference to free speech interests, a court will not grant an injunction restraining the publication of an allegedly defamatory article if the publisher asserts that he will be invoking a defence at

---

16 Anthony Lester, "Freedom of Expression: Relevant International Principles" in *Developing Human Rights Jurisprudence* (Commonwealth Secretariat, 1988), at 44.

17 Raymond Wacks, *op cit*, at 162.

the trial. The first of these defences is "absolute privilege". This accords complete immunity from suit when made in the course of parliamentary or judicial proceedings, high executive communications and marital communications. "Qualified privilege" protects defamatory communications made in certain situations such as when it is made:

(i) in the discharge of some public or private duty to someone with a reciprocal duty in receiving it, such as reporting a crime;

(ii) for the protection of the maker's own interests to a person with a corresponding duty to receive it, such as an employee's response to his superior regarding a complaint; or

(iii) on a subject where the maker and the recipient share a legitimate interest, such as superiors discussing a subordinate.

18.30 The privilege arising from these categories of communications is "qualified" in that the protection is forfeited if the communication is not made to serve the legitimate purpose of the privileged occasion, but instead some ulterior motive.

18.31 Absolute and qualified privilege apply to the media and ordinary citizens alike, but have been slightly extended for the media in respect of fair and accurate press reports of the proceedings of a wide range of bodies such as courts, statutory bodies and company general meetings.

18.32 It is, however, the defence of "fair comment" which evinces English defamation law's most significant concession to free speech. While well-intentioned but factually inaccurate defamatory statements on matters of public interest are unprotected, "fair comment" on such matters is protected. The statement must accordingly qualify as a comment, rather than a statement of fact, yet be sufficiently based on fact to qualify as "fair". It must also be made "on a matter of public interest". In the present context, it is relevant that in many cases judges have emphasised the importance of protecting free comment on issues of current political interest.

Contempt of court

18.33 Contempt of court is the unwarranted interference with the administration of justice. It particularly affects the media's capacity to give pre-trial publicity to trials which are of public interest. Such publicity constitutes a contempt if it creates a real risk of influencing the outcome of the trial. As such it inhibits free speech, which the doctrine holds must defer to the requirements of justice.

Breach of confidence

18.34 It will be recalled that this is a civil remedy affording protection against the disclosure or use of information, including personal information, which is not publicly known and is entrusted in circumstances giving rise to the duty of confidence. As Professor Wacks points out "such an obligation will normally arise when information is imparted (either explicitly or implicitly) for a limited purpose".[18] It accordingly has a similar content as the Use Limitation Principle. The obligation of confidence attaches not only to the original recipient, but also to those subsequently receiving it who become aware that it was originally imparted in confidence. Our analysis in Chapter 4 concludes that the principle affords only limited protection to privacy, as compared to the Use Limitation Principle for, unlike the latter, it can only be enforced by the original discloser and not (unless he is one and the same) the individual to whom it relates.

18.35 The other side of the coin is that the duty of confidence can be used as a curb on free speech, particularly when deployed in conjunction with contempt of court. This is largely due to the readiness with which an interim injunction is granted. Unlike a defamation suit, the plaintiff seeking the injunction must only show an arguable case, but by the time the matter has come to trial the information is likely to have lost its news value. This was the position in *Spycatcher* before the House of Lords. In that case the *Guardian* ran a news story referring to Peter Wright's allegations. The government obtained an interim injunction against the newspaper repeating the story prior to trial. Before the trial the *Independent* came into possession of more detailed allegations and published them. The paper was then prosecuted for contempt of court for flouting the spirit of the injunction. Robertson and Nicol comment that:

> *"[This doctrine] requires newspapers who wish to publish stories about a matter some aspect of which is affected by an injunction against another publication to apply to the court for guidance on whether their story trespasses upon the order in existence - a procedure calculated to give High Court judges a good deal of experience in editing newspapers."*[19]

18.36 In the subsequent appeal, the European Court held that an interim injunction constitutes a form of "prior restraint" whose compatibility with the Convention's free speech provision required "the most careful scrutiny". In the event, 14 of the 24 judges held that the initial injunctions did not violate the Convention, indicating that the decision on this point is close to the limits of acceptability under the Convention. The Court further held, unanimously, that the injunctions contravened the Convention upon the confidentiality being destroyed by its publication in the USA.

18.37 The breach of confidence action does therefore possess the potential to inhibit free speech. This is mitigated, however, by the fact that, if

---

18 Wacks, in Meron (ed), *op cit*, at 52.

19 Geoffrey Robertson & Andrew Nicol, *Media Law* (Longman, 1990), at 18.

the plaintiff is the government, it is a defence that the disclosure is in the public interest.

Administrative remedies: self regulation

18.38 In Hong Kong, therefore, the legal actions of defamation and breach of confidence afford some incidental protection to privacy. Their accessibility and utility is restricted, however. Administrative remedies are therefore an attractive remedy. Approximately 20% of journalists are members of the Hong Kong Journalists Association. The Association has promulgated a code of ethics and complaints are handled by a special ethics committee. Although the code of ethics has binding effect only on HKJA's own members, in reality it has been widely adopted and accepted by the profession as a whole. For present purposes, the relevant provisions of the Code are the following:

> *"3. A journalist shall strive to ensure that the information he/she disseminates is fair and accurate, avoid the expression of comment and conjecture as established fact and falsification, by distortion, selection or misrepresentation.*
>
> *4. A journalist shall rectify promptly any harmful inaccuracies, ensure that correction and apologies receive due prominence and afford the right of reply to persons criticised when the issue is of sufficient importance.*
>
> *5. A journalist shall obtain information, photographs and illustrations only by straight forward means. The use of other means can be justified only by over-riding considerations of the public interest. The journalist is entitled to exercise a personal conscientious objection to the use of such means."*

18.39 Although the code does not refer to privacy interests as such, they have figured in the ethics committee's deliberations on the coverage of such issues as student suicides.

18.40 In the United Kingdom a more elaborate self-regulatory scheme appears to have failed. We recognize, however, that the local media culture is a crucial determinant of the success of self-regulation schemes. As Wong Kwok-wah, a member of the sub-committee has pointed out, the Swedish Press Council is arguably the most successful example self-regulation in the world, yet its composition and powers are similar to its failed British counterpart. This issue will be considered in more detail in the second part of our reference when we will examine the need for a specific remedy for public disclosure infringing privacy interests. It is less relevant to the present issue

of the extent to which the media should be exempted from the data protection principles in the light of existing legal and administrative remedies.

Statutory constraints on free speech

18.41 To complete this overview of the general legal context in which the Hong Kong media operates, reference is required to a number of statutory constraints which operate to inhibit the media's capacity to report what it likes and what the public may wish to read and hear. These are summarised in *Urgent Business,* [20] the Joint Report of Article 19 and the Hong Kong Journalists Association. They total 17 and include the Official Secrets Act, the sedition provision of the Crimes Ordinance (Cap. 200), the Broadcasting Authority Ordinance (Cap. 391), the Television Ordinance (Cap. 52), the Telecommunications Ordinance (Cap. 106), the Film Censorship Ordinance (Cap. 392), and the Places of Public Entertainment Ordinance (Cap. 172). The Government has undertaken a comprehensive programme of review of all these and 10 other ordinances not identified by the HKJA. Three ordinances have been amended and amendments for two others have been introduced into the Legislative Council. The review process is scheduled for completion within two years.

Application of the data protection principles to the media

18.42 It emerges from the above that only incidental legal protection is currently afforded against media intrusions, through the common law remedies of defamation and breach of confidence. There is also a restricted administrative remedy available through the Hong Kong Journalists Association. On the other hand, there are a large number of existing constraints on free speech, including the converse operation of the two common law remedies. The cumulative effect of these provisions is to further shrink the parameters of legally permissible disclosures. It is against this background that we now individually assess the application of the data protection principles to the media.

Data protection and privacy interests distinguished

18.43 Although the decisions cited above, particularly *Winer*, indicate the appropriate relationship between free speech and privacy, their application to data protection requires further analysis. *Winer* indicates that the media's free speech rights must only be qualified to the strict extent necessary to preclude serious invasions of privacy. However, the data protection principles are more expansive than the ambit of the right to privacy under the Bill of Rights, although there are common elements. The most important difference is that the privacy right is restricted to information

[20] Hong Kong Journalists Association & Article 19, *Urgent Business* : *Hong Kong, Freedom of Expression and 1997* (1993).

pertaining to one's "private life", whereas data protection attaches to *any* information relating to an identifiable individual. More generally, the data protection principles do not restrict themselves specifically to privacy concerns, as they also represent fair information practices. However, those principles attending solely to data management issues, such as data security, will not inhibit free expression. It is not therefore possible to make an overall assessment of the interaction of the data protection principles and free speech. As the Council of Europe has pointed out, outright inclusion or exclusion of the media from the data protection regime would lack the necessary proportionality required by human rights law. Accordingly, we have assessed the extent to which each of the principles could inhibit free speech by the media.

Security Safeguards Principle

18.44 Application of this principle to the media would not affect the free speech rights of the media. We note that in several countries, such as Germany and Austria, it is the only data protection principle applied to the media.

The Collection Limitation Principle

18.45 This requires that the collection of data should be limited to that relevant to the functions of the collector. This limitation does not restrict the media as its function is the collection information for the purposes of publication.

18.46 The principle goes on to require fair collection and the question arises whether this would unduly inhibit the media, particularly when engaged in investigative journalism. "Fairness" is a flexible notion and it is relevant that the Bill of Rights free speech provision goes further than the European Convention in its emphasis on active journalism. Whereas the Convention states that the right includes receiving and imparting information and ideas, the Bill of Rights provision adds reference to the freedom to *seek* the same. Kevin Boyle[21] points out that the preparatory documents of the Covenant from which the provision derives reveal that "seek" was chosen instead of "gather" to connote an active process of collecting information rather than one restricted to the passive acceptance of information provided by others.

18.47 As pointed out previously, "fairness" is a flexible notion. It follows from the above that what is "fair" for a news-gathering investigative journalist may be less so for an individual not so engaged. We think that this flexibility should be sufficient to accommodate the media. On this basis we recommend that the principle of fair collection should apply to the media.

---

[21] Kevin Boyle "The Right to Freedom of Opinion and Expression" in Yash Ghai & Johannes Chan (eds), *The Hong Kong Bill of Rights : A Comparative Approach* (Butterworth, 1992).

18.48 As regards the remaining requirement that collection be "lawful", we note that there are at present few ordinances restricting the collection of data. We will be examining this aspect in greater detail in the second part of our reference, and envisage recommending more specific legal controls on the surreptitious collection of data by means of such methods as phone tapping and eavesdropping. We will also have to consider at that stage the scope of exemptions required to accommodate competing social interests, including free speech. In the meantime, however, we see no justification for the media not complying with such laws as presently apply. We note that this is the position even in the United States, with its pronounced press freedoms. Its Supreme Court has consistently held that the Constitution's First Amendment does not "accord newsmen immunity for torts or crimes committed during the course of newsgathering. The First Amendment is not a licence to trespass, to steal, or to intrude".[22] **We conclude that the Collection Limitation Principle should apply in full to the media.**

Data Quality Principle

18.49 This requires that data should be accurate and complete. We recommended the qualification, however, that data users should not be liable for compensation where the inaccurate data nonetheless accurately records data received from another and that the data are identified as such. This limitation would provide the media with a protective shield not available to it in defamation claims. We do not, therefore, anticipate that this aspect of the principle will present the media with any difficulties.

18.50 More difficult is the remaining aspect, namely that data should be "up-to-date". This is usually vital, because it is on the basis of their data that decision-makers affect the individual. But the media has a different relationship to its data as compared with other data users. The only decision it may make affecting the data subject is whether to publish. We have considered this aspect of the matter further and have concluded that, given the particular circumstances of the media's use of personal data, it is not necessary to qualify the Data Quality Principle. This differs from the view originally expressed in the Consultative Document. The Data Quality Principle only requires that data be accurate to the extent necessary for the purpose for which the data are held. As the data are held for the purpose of publication, we believe that it is inherent in the Data Quality Principle that the data need only be accurate at the time of publication. **We accordingly recommend that the Data Quality Principle apply without qualification to the media.** One further consideration is whether the media should be required to publish a correction to inaccurate published data. The Hong Kong Journalists Association argued against such an obligation and pointed to the difficulty in some cases of distinguishing fact from opinion. We have concluded that the same requirement should be imposed on the media in respect of disseminated inaccurate data as applies to others. **We recommend that the media be required to take all practicable steps to**

[22] See note 1, at 237.

disseminate a correction where inaccurate data has been published. It would be up to the publisher to decide how best this could be achieved.

Purpose Limitation and Use Limitation Principles

18.51 The combined effect of these two principles is that data should not be published unless it is either specifically obtained for that purpose, or the data subject's consent is obtained. The latter is an unrealistic possibility with most public disclosures. The very process of attempting to obtain consent would constitute an unacceptably potent form of prior restraint.

18.52 The more difficult issue is whether the media should only publish data consistently with the purpose for which it was obtained. This is not likely to present problems regarding data obtained by the media. Unlike many data users, the media has a single, specific purpose, namely obtaining data for the purposes of publication. This purpose is therefore likely to be in the contemplation of both those providing data to the media and to the journalists receiving it. This does not conclude the matter, however, as the two principles would equally apply to informants passing on the data to the press. These principles would restrict prospective sources from passing on information to the media, for informants are unlikely to obtain the data with the specific purpose of aiding in its publication. This is particularly so when the data discloses illegality or impropriety. Yet such data is particularly likely to be of public concern. The media, and hence the public, is largely dependant on "whistleblowers". To pillory such persons would inhibit the dissemination of information of public importance. We have noted that in breach of confidence actions there is a general public interest defence to suits brought by government. In view of these considerations **we recommend an exemption from the Use Limitation Principle for data the publication of which is in the public interest.**

18.53 The remaining question is what constitutes the "public interest". We have considered whether the "public interest" should be spelt out. We note that this is the approach that has been adopted by the Australian Law Reform Commission[23], the Calcutt Committee[24], and most recently the Lord Chancellor[25]. Our difficulty has been in formulating a general harm test that both identifies and sufficiently demarcates the conduct to be covered. One option would be to define "public interest" by reference to the prevention or remedying of specific conduct, such as publicising seriously anti-social conduct or misrepresentations by public figures. This was the approach adopted by Sir David Calcutt in formulating a defence to a proposed tort action against the media. Upon further reflection, and in the broader context of a data protection law, we think that such an approach runs the risk of unnecessarily removing flexibility from the law to deal with changing circumstances and values. We have therefore concluded that the question of

---

23 Australia Law Reform Commission, *Privacy* (Report No. 22) Canberra 1983.

24 See note 3.

25 Lord Chancellors Office, *Infringement of Privacy*, HMSO 1993.

what is in the public interest should be left to the independent judiciary to decide.

18.54 A perennial problem in determining the scope of a public disclosure is differentiating that information which is "of public interest" from that which is merely interesting to the public. The latter would encompass the gratuitous or sensationalist revelations about an individual. The distinction is more equivocal than is sometimes suggested, but we are satisfied that the courts will be alert to exclude matters which are not of genuine public concern.

18.55 It has been pointed out in the context of a breach of confidence case that:

> *"In certain circumstances the public interest may be better served by a limited form of publication perhaps to the police or some other authority who can follow up a suspicion that wrongdoing may lurk beneath the cloak of confidence."*[26]

18.56 The difficulty is that qualifying the application of the exemption to accommodate this point would be very difficult. For one thing, it would be necessary to cover the situation where there were reasonable grounds for suspecting that the appropriate investigative agency was not disposed to follow the matter up adequately. In those cases where it is clearly appropriate to alert such a body we think it reasonable to assume that the media will arrange this.

18.57 In addition to an exemption which enables media informants to reveal illegal or seriously anti-social conduct, we also think that an additional exemption is necessary which attends to the specific role of the media in publicizing matters of concern. In this regard, we adopt the additional test proposed by Sir David Calcutt as a defence to a tort action against the media when it has sought to expose the misrepresentations of a public figure. **We recommend adoption of the Calcutt formulation that an exemption be provided "for the purpose of preventing the public from being misled by some public statement or action of the individual concerned."**

The Openness and Individual Participation Principles

18.58 These principles provide individuals with access to data pertaining to them and the right to correct that data. They have a benign application in most spheres. They enable the data subject to monitor and improve the quality of data concerning him. We have recommended that data subjects have at least indirect access to all data except that held for the purposes of security, defence, and international relations in respect of Hong Kong. Like the restriction of data purposes, access to personal data (more particularly if it relates to one's private life) is a protected right under the Bill of Rights. The issue is whether according these rights could unduly inhibit press

---

[26] *AG v Guardian Newspapers* (No. 2) [1988]3 WLR 776 at 794, per Lord Goff.

freedom. There are two levels where this could arguably occur. The first is that at the operational level the activities of the media would be seriously affected by fulfilling access and correction rights and that they would act as a form of prior restraint. The second is that at the institutional level, the Privacy Commissioner's involvement in access and correction mechanisms is inconsistent with the autonomy required of a free press.

Access and correction rights: operational difficulties

18.59 The Hong Kong Journalists Association has objected that if no exemption is accorded to the media in respect of access to its unpublished data, its activities would be fundamentally undermined in the following respects:

(a) it would undermine investigative journalism. Individuals concerned that their (possibly improper) activities might attract media attention would be able to obtain access to journalistic data held at that stage. The HKJA fears that this could result in a court injunction to kill the story. Alternatively, the individual may well be able to anticipate future lines of inquiry and have potential sources "warned off' before the journalist is able to contact them. Granting pre-publication access and correction rights could generally usurp the publication process, by tying up resources and delaying publication. The "truth" of press assertions may be anything but cut and dried, as they will often comprise a complex mix of opinions and interpretations. Imposing access rights could have the opposite effect to that intended by prompting premature publication to beat the lodgement of access and correction requests.

(b) access could lead to the revelation of confidential sources. The submission states that "any attempt to infringe upon the well-recognised principle of non-disclosure of sources would cause irreparable harm to the ability of the profession to carry out its duties on behalf of the public." However, confidentiality of sources is important for many data users, such as law enforcement and regulatory authorities. We have considered it sufficient to qualify access rights accordingly, with the mediation of the Privacy Commissioner. The argument that the Privacy Commissioner should be denied a role mediating the access mechanism would presumably be based on the fact that media sources are more likely to be at loggerheads with the administration. As such it is addressed in the institutional argument against access developed below.

Access rights: institutional problems

18.60 At the second level, there is an argument that subjecting the media to data subject access and correction rights would, to the extent that they are mediated by the Privacy Commissioner, undermine the media's institutional integrity. This concern is not articulated by the HKJA, but it is suggested by Baker's useful distinction between "defensive" and "offensive" rights of the media. He defines defensive rights as those that "protect the institution (or reporters and press corps) from destruction, interference, or appropriation by government. They include testimonial privileges, protection against search and seizures, and most protections against regulations that are directed particularly against the press". He argues that these defensive rights are essential if the press is to discharge the watchdog role incumbent upon it:

> *"To operate as a check on government, the press must have some independence from it. Such independence implies effective defence against governmental intrusions ... Even well-intentioned regulations designed to further the government's conception of a properly functioning responsible press, such as public access rights or right-to-reply rules, may undermine press independence. They would restrict the way the press packaged and conceptualized its message, its potential expose. Likewise, government practices that are designed to address public concerns and that affect media and non-media alike can weaken the press's institutional integrity".*[27]

18.61 It is to be noted that Baker's concern with government controls does not assume that they will be exercised malignly. His argument is that no matter how well intentioned, they tend to negate the media's independence. The point at which the applicability of his analysis may be questioned, however, is its focus on government interference. As we make clear in Chapter 16, we have endeavoured to constitute the Privacy Commissioner as being independent of government. Such independence is vital if he is adequately to carry out his role of regulating government use of personal data. Nonetheless, there are precedents in other jurisdictions for the government endeavouring to put pressure on ostensibly independent agencies. Flaherty documents instances where the governments of well established democratic governments have brought pressure to bear on Privacy Commissioners.[28] Certainly, should such a situation arise here, the media's watchdog role would be made more vulnerable by a mechanism legitimating officials examining its holdings.

18.62 We are also aware that even if journalistic fears of official reprisals are unfounded, they could result in the inhibiting or "chilling" of journalistic enterprise. It is important to avoid establishing regulatory mechanisms which will convey to journalists a restriction of their liberty.

---

27 See note 1, at 237.

28 David Flaherty, *Protecting Privacy in Surveillance Societies* (University of North Carolina press, 1989).

Recommendation on pre-publication access and correction lights

18.63 Throughout this report our fundamental concern is with data exposing the individual to adverse decisions. The sole journalistic decision to this effect is to publish. Whilst the consequences of this may drastically affect the individual, we have concluded that to accord access and correction rights at the pre-publication stage would unduly inhibit journalists in the exercise of their essential tasks. **We accordingly recommend an exemption from the principles according access and correction rights for unpublished data held by the media solely for journalistic purposes. This exemption should extend to indirect access through the Privacy Commissioner.** In making this recommendation, we acknowledge that "publication" and "journalistic purposes" will require definition.

18.64 More difficult is the issue of the publication of corrections. This raises complex questions regarding the potential of such a mechanism to constitute a form of post-publication censorship. As such, we will defer its consideration to our further report on the media and privacy. These prior-constraint problems do not extend to unpublished corrections of journalistic records following publication. Accordingly the exemption does not extend beyond the data's publication.

Pro-active investigations

18.65 We have recommended that the Privacy Commissioner should be entitled not only to investigate complaints received, but to initiate such investigations and to conduct on-site inspections of data users. We have further recommended that in the carrying out of these duties, he may enter premises but, if he does not obtain consent to such entry, a court order is necessary. We consider that the requirement of court approval sufficiently counters the danger of abuse. The seizure of evidence we have recommended be governed by a provision along the lines of Cap. 397.

18.66 For reasons spelt out above, we prefer that the Privacy Commissioner perform a purely reactive role in his monitoring of the media. **We accordingly recommend that he be restricted to the reactive role of investigating complaints about the media.**

Administrative compliance: declarations

18.67 We have recommended that all private sector data users be required to lodge a declaration specifying the purposes for which they hold data, a description of any sensitive categories of data held, and contact details of the responsible officer. Public sector data users will be expected to lodge more comprehensive declarations. We have proposed that this requirement apply to all organizations using data, whether or not some of their

data purposes are partially exempted from compliance with the data protection principles. In the case of the media, we expect that they will also be engaged in routine uses, such as personnel management. As with other data users, their declaration should not be restricted to these, however, but should also identify those data purposes for which exemptions are claimed. Secret databases negate the requirement of data transparency. **We accordingly recommend that the declaration requirement also apply to the media.** Employee journalists will be covered by their employer fulfilling this requirement.

Additional protection measures against media intrusions

18.68 This report is concerned with the application of the data protection principles. As they represent internationally recognized fair information practices we have proceeded on the general basis that their application to particular sectors does not require specific justification. Rather, exemptions for specific data purposes require justification. A similar approach was adopted when examining the exemptions necessary for other competing social interests, such as law enforcement. As the OECD emphasizes, exemptions "should be as few as possible".

18.69 In the next part of the reference we will be examining the need for additional legal remedies to deal specifically with public disclosures infringing privacy. The data protection principles do not address the essential complaint arising from media intrusion, namely the disclosure of correct data in circumstances where it constitutes an unjustified intrusion into an individual's private life. As Professor Wacks points out, "if 'personal information' and 'press freedom' are to be given proper recognition and protection, the determination of actionability for unauthorized publicity ought to depend on the separation of the two inquiries".[29] We will also have to address the question of whether additional administrative or legal remedies are necessary. This will require a wider enquiry than has been necessary here. In particular, it will be relevant to establish the extent to which there exists a problem of the Hong Kong media intruding on privacy and the adequacy of existing remedies. Also relevant will be public attitudes on the question. In this regard we note the results of surveys conducted last year by "Eastweek"[30] magazine and Dr John Bacon-Shone of the sub-committee.[31]

---

29 See note 16, at 159.

30 *Eastweek* 20 May 1993.

31 See Appendix 2.

Appendix 1

Organisations/Individuals from whom Submissions on the Consultative Document were received

ASM Group
American Express
Attorney General's Chambers, International Law Division
Bennett, Colin J, Associate Professor, Department of Political Science, University of Victoria
Buildings and Lands Department
Caritas Hong Kong
Chase Manhattan Bank, N.A.
Chinese General Chamber of Commerce
Chinese Manufacturers' Association of Hong Kong
Citibank, N.A.
Civil Aviation Department
Civil Service Branch
Consumer Council
Correctional Services Department
Data Protection Registrar, UK
Datatrade Ltd
Dresner, Stewart
Economist
Employers' Federation of Hong Kong
Far East Trade Press Ltd
Financial Services Branch
Health and Welfare Branch
Holland, Kevin, Chairman of Data Protection Committee, The Advertising Association (UK)
Association of Banks
Bar Association
Hong Kong Christian Service
Hong Kong Coalition of Service Industries
Hong Kong Committee for UNICEF (UN Children's Fund)
Hong Kong Computer Society
Hong Kong Council of Social Service
Hong Kong Direct Marketing Association
Hong Kong Export Credit Insurance Corporation
Hong Kong Federation of Insurers
Hong Kong Housing Authority & Housing Department
Hong Kong Human Rights Commission
Hong Kong Institute of Engineers
Hong Kong Institute of Personnel Management
Hong Kong Journalists Association

Hong Kong Medical Association
Hong Kong Monetary Authority
Hong Kong Polytechnic
Hong Kong Trade Development Council
Hospital Authority
Immigration Department
Independent Commission Against Corruption
Information Technology Services Department
Inland Revenue Department
Institute of Chartered Secretaries & Administrators – HK
Labour Department
Land Registry
Lee, Wanbil W, Head of Department of Computer Studies, Lingnan College
Madsen, Wayne, Integrated Systems Division, Computer Sciences Corporation (USA)
Mailing List (Asia) Ltd
Office of the Commissioner of Insurance
Oxfam - Hong Kong
Phillips, Bruce, Privacy Commissioner of Canada
Planning, Environment and Lands Branch
Post Office
Rating and Valuation Department
Reader's Digest
Regional Services Department
Registrar General's Department
Registry of Trade Unions
Riley, Thomas, Riley Information Services Inc. (Canada)
Royal Hong Kong Police Force
Securities and Futures Commission
Security Branch
Social Welfare Department
Society of Homes for the Handicapped
Society of Hong Kong Publishers Ltd
Stock Exchange of Hong Kong Ltd
Strategic Solutions
Student Financial Assistance Agency
Swire Properties Ltd
Trade and Industry Branch
Transport Department
Treasury
United Democrats of Hong Kong
University of Hong Kong
Urban Services Department
Vocational Training Council
Works Branch

Appendix 2

Summary of the Results of the Survey on Privacy Attitudes in Hong Kong conducted by Dr. John Bacon-Shone and Harold Traver

[This study was wholly funded by the Conference and Research Grants Committee of the University of Hong Kong. The summary below of the survey results was prepared by Dr. John Bacon-Shone. The text of the questionnaire follows the summary.]

"This study aims to provide information about the attitudes of the Hong Kong public with regard to privacy, encompassing data protection, privacy & the media and surveillance. The only previous academic study of privacy in Hong Kong was done by one of us (HT) 15 years ago, and as such is now out-of-date. In addition, the focus of the previous study was on different aspects of privacy. The only other study in Hong Kong that we are aware of is a small study done recently by the SSRC for Eastweek magazine .....

..... The survey used several different approaches. One was to try to assess whether respondents were aware of a breach of their privacy (with respect to personal data) within the last 12 months, and if so, to try and collect some limited data about this breach. Secondly, we attempted to identify what sorts of personal data respondents considered sensitive, for themselves, for politicians and for film stars. Thirdly, we presented a number of practical situations that we felt respondents might relate to. We asked how concerned respondents were about these situations, and whether they felt control was needed. Fourthly, we checked on attitudes to a number of social problems including privacy. Lastly, we collected demographic information .....

Privacy incidents:

A total of 7.3% of the sample had experienced an invasion of their privacy within the last 12 months. This was defined as someone having tried to learn too much about them. About one fifth of these respondents (1.5% overall) had been very concerned about the incident. While 1.5% seems a very small proportion, even if we take a statistically very conservative approach and use 0.5% which represents the smallest proportion that is consistent with our sample (using a 95% confidence interval), this still represents more than 20,000 people when projected to the population. If so many people have serious invasions of their privacy each year, this suggests that a serious problem does indeed exist, despite the small attention given to it in the media.

Personal Data:

Respondents were given a list of types of personal data and asked whether they would object if this information was made publicly available to anyone who wanted it, firstly if it was their own data, secondly if it was data for a politician and lastly for a film star.

	Self	Politician	Star
Address	83.8	60.8	79.0
Telephone No.	86.3	67.9	79.2
Photo	87.5	30.2	25.8
Photo (intimate & private)	85.4	62.9	56.3
Political views	42.5	20.6	28.1
Religious views	15.2	15.8	20.6
Income	58.3	40.4	52.9
Medical history	57.3	46.9	55.0
I.D. Card No.	62.9	45.0	54.8
Financial status	63.7	43.3	53.1
HIV status	62.7	50.2	57.5
Passport/Nationality	23.3	21.2	28.8

Numbers are percentages of respondents who would object.

Perhaps surprisingly, the overwhelming majority of respondents considered that their address, telephone number and photograph should not be freely available. It is necessary to explain to those who are unfamiliar with Hong Kong that because of the presence of homonyms and the limited number of Chinese names, it may be hard to find out someone's telephone number unless you know their address as well as the written version of their name. Interestingly, a majority considered that the address and telephone number of politicians should not be public, and an overwhelming majority considered that the address and telephone number of a star should be restricted. Not surprisingly, most people saw no reason why the photos of politicians or stars should be restricted unless the photos were intimate and taken in a private place.

As regards income, medical history, ID car no., financial status an HIV status, a small majority was against public access to this data regarding politicians, except for HIV status.

There was very little concern over religious views or nationality, with some concern over political views (mainly for self). Any conclusion regarding nationality should probably by treated with some caution as it may be that the reason for the lack of sensitivity is because the vast majority of Hong Kong people do not have a foreign passport.

In summary, what is perceived by the public as sensitive data in specific to Hong Kong, and it is clear that Hong Kong people do feel strongly that much of their personal data should not be publicly available.

Privacy Situations

It is clear from the responses to situations that Hong Kong people are very concerned over some privacy issues, and have little concern over others. A summary is as follows:

Situation	Very concerned/extremely worried	Need Control
See into your flat	64.9	68.8
Telephoto Pictures	87.5	87.6
Employer opens mail	86.6	79.3
Police tap any phones	42.7	59.0
Telephone in paper	42.9	72.2
Tax info available	53.7	66.5
ID card for cheque	19.5	29.1
ID card for change US$100	18.0	21.7
Debt notice	81.9	89.2
Credit Check (informed)	33.9	45.7
Credit Check (uninformed)	44.0	56.4

	Should have Right
Loan refused (right access)	84.5
Loan refused (right correction)	94.0
Stop direct mail	62.9

All numbers are percentages of those who held a view.

Clearly, the only issues for which there was little concern or demand for control was over the use of ID card numbers, possibly reflecting recognition of the efficiency associated with the their use in Hong Kong and/or excess familiarity with the situation. However, it is important to relate the lack of concern over the use of ID card numbers to the concern of the majority that their ID card number was till sensitive data.

Views are divided over the need for control of phone tapping by the police and of credit checks.

For all the other issues there is clear support for some control mechanism, with notably the right of correction after a loan refusal attracting a positive response of 94% and control of debt collecting notices attracting a 89% positive response.

It seems to be a reasonable conclusion that the public supports controls in many of the areas where the LRC proposals are likely to have a major impact.

Social Attitudes

In this section of the questionnaire, we took some of the social issues that are generally seen as important by the HK public, to provide a comparison with privacy issues. A crude summary shows:

	Very Important	Somewhat or Very Important
Pollution	54.9	95.6
Corruption	44.5	81.8
Law & Order	55.1	90.1
Privacy	25.4	66.8
Housing	61.7	91.8
Inflation	52.8	94.0
Public Confidence	35.9	78.0

All numbers are percentages of those responding.

This indicates, not surprisingly, that privacy is seen as very important by many fewer respondents than the other issues, but conversely, it is still seen as very important by a quarter of respondents and as at least somewhat important by two thirds. This may be seen as surprisingly high, given how much less media and political attention has been paid to this issue than all of the others .....

Survey Methodology

This survey was a telephone survey of adults (aged 18 years or above) and should be broadly representative of all Hong Kong households (except for the 1% or less who do not have a telephone). Adults were selected randomly within the household on the basis of the last birthday. The major sources of bias are likely to be non-contacts and refusals. We made five attempts to contact each telephone number before giving up. The overall results for all telephone numbers tried are:

Label	Count	Percent
Success	520	19.16%
Partial	34	1.25%
Refusal	816	30.07%
Language problem	11	0.41%
Fail to qualify	73	2.69%
Business	93	3.43%
Not in	31	1.14%
No Answer	666	24.54%
Busy	55	2.03%
Fax/Data	86	3.17%
Invalid	324	11.94%
Answering Machine	5	0.18%
Total	2714	100.00%

Thus the success rate amongst those contacted who qualified is 520/(520+34+816)=38%, which is somewhat lower than the normal 50-60% success rate in the SSRC. This is likely to be at least partially due to the relatively long and demanding questionnaire on a topic that may not appear at first to be of great interest."

Text of the Questionnaire

"Introduction

This survey is being done by the Social Sciences Research Centre, HKU regarding possible changes in the law on data protection and privacy. This will be an important source of information for the Law Reform Commission to assist in recommending improvements in law to the Hong Kong Government. This survey is confidential and no attempt will be made to identify respondents.

V3. Is there any member in your family over 18?
1. Yes
2. No (if none, terminate the interview)

If more than one, may I speak to the one who will have his/her birthday next?

V4. Which district are you living in?
1. Wanchai
2. Eastern
3. Central & Western
4. Southern
5. Kwun Tong
6. Kowloon City
7. Wong Tai Sin
8. Mongkok
9. Sham Shui Po
10. Yau Tsim
11. Sai Kung
12. Shatin
13. Islands
14. Tsuen Wan
15. Kwai Tsing
16. Tuen Mun
17. Yuen Long
18. North
19. Tai Po
20. No answer

V5. Including yourself, how many people are there in your household?

V6. What is your sex?

1. Male
2. Female

V7. Could you tell me the type of housing in which you are living?
1. Public Housing Estate
2. Home Ownership Scheme
3. Private Flats
4. Village Type
5. No answer

V8. Approximately how large is your living area?

V9. Are you working in government department, a public body, or a private firm?
1. A government department
2. A public body (eg MTRC, KCRC)
3. A private firm (go to V10)
4. Self-employed
5. Not applicable - not working
6. No answer/Don't know

V10. Approximately how many employees are there in your company?

V11. What is your occupation and position?
1. Managers and Administrators
2. Professionals
3. Associate Professionals
4. Clerks
5. Service Workers and Shops Sales Workers
6. Skilled Agriculture and Fishery Workers
7. Craft and Machine Operators and Assembles
8. Plant and Machine Operators and Assembles
9. Non-skilled Workers
10. Student
11. Housewife
12. Unclassified
13. Others (unemployed, retired, etc)

V12. What is your average total monthly personal income including those incomes such as rent, interest etc?
Enter amount (to nearest $1k if possible)

I am going to read to you seven problems which some people say are affecting Hong Kong. For each please indicate whether you think these problems are very important, quite important, not very important or not at all important.

V13. Pollution of the environment
1. Very important
2. Somewhat important

3. Not very important
4. Not at all important
5. No answer/Don't know

V14. Corruption of either government or business
1. Very important
2. Somewhat important
3. Not very important
4. Not at all important
5. No answer/Don't know

V15. Breakdown of Law and Order
1. Very important
2. Somewhat important
3. Not very important
4. Not at all important
5. No answer/Don't know

V16. The intrusion of business or government in individuals' privacy
1. Very important
2. Somewhat important
3. Not very important
4. Not at all important
5. No answer/Don't know

V17. The high cost of housing
1. Very important
2. Somewhat important
3. Not very important
4. Not at all important
5. No answer/Don't know

V18. Rising inflation
1. Very important
2. Somewhat important
3. Not very important
4. Not at all important
5. No answer/Don't know

V19. A decline in public confidence about the future of Hong Kong
1. Very important
2. Somewhat important
3. Not very important
4. Not at all important
5. No answer/Don't know

V20. I would like to ask you about how you would feel if certain types of information were publicly available you. Would you object to any of the following information about you being publicly available?
1. Your address
5. Your political views

2. Your telephone no.
3. Your photo
4. Your photograph being intimate with a non-family member in a private place
6. Your religious views
7. Your income
8. Your medical history
9. Your I.D. card no.
10. Your financial status
11. Your HIV status
12. Your passport/nationality(ies)

[Multicode] Answer:_____

V21. Now, would you object to any of the following information about a politician (eg Martin Lee, Allen Lee) being made available regardless of their wishes?

1. Their address
2. Their telephone no.
3. Their photo
4. Their photograph being intimate with a non-family member in a private place
5. Their political views
6. Their religious views
7. Their income
8. Their medical history
9. Their I.D. card no.
10. Their financial status
11. Their HIV status
12. Their passport/nationality(ies)

[Multicode] Answer:_____

V22. How about a movie star regardless of their wishes? (eg DoDo Cheng, Chow Yun Fat)

1. Their address
2. Their telephone no.
3. Their photo
4. Their photograph being intimate with a non-family member in a private place
5. Their political views
6. Their religious views
7. Their income
8. Their medical history
9. Their I.D. card no.
10. Their financial status
11. Their HIV status
12. Their passport/nationality(ies)

[Multicode] Answer:_____

V23. Has there been any time in the last 12 months when you felt that someone or some organisation wanted to know too much about your private and personal affairs or the private affairs of your family?

1. Yes
2. No (go to V33)

V24. Can you tell me what happened?

_____
_____

V25. Who was responsible for this?_____

V26. How many months ago did it start?

V27. How long did it last

1. Still going on

2. Up to 1 month
3. Up to 3 months
4. Up to 6 months
5. Up to 12 months

V28. Did you take this as a serious matter?
1. No concern at all
2. Little concern
3. Very concerned
4. Extremely worried

V29. Have you taken any action?
1. Yes
2. No (skip to V32)

V30. What action did you take?_____

V31. Did this make it stop?
1. No, continued
2. Yes, stopped

V32. Do you think it is necessary that this should be controlled or limited by law?
1. Yes
2. No
3. Don't know

Rubric
I am now going to present a number of situations and for each situation, I would like you to tell me how serious you take the matter and whether you think there should be legal protection:-

V33. Recently a building has been built so close to yours, that people in it can easily see what you are doing in your living room. Do you take this as a serious matter?
1. No concern at all
2. Little concern
3. Very concerned
4. Extremely worried

V34. Do you think it is necessary that this should be controlled or limited by law?
1. Yes
2. No
3. Don't know

V35. Someone uses a camera with telephoto lens to take a picture of you in your house without your knowledge or consent. Do you take this as a serious matter?
1. No concerned

2. Little concern
3. Very concerned
4. Extremely worried

V36. Do you think it is necessary that this should be controlled or limited by law?
1. Yes
2. No
3. Don't know

V37. You discover that your employer has been opening mail sent to you marked "personal". Do you take this as a serious matter?
1. No concern at all
2. Little concern
3. Very concerned
4. Extremely worried

V38. Do you think it is necessary that this should be controlled or limited by law?
1. Yes
2. No
3. Don't know

V39. You read in the newspaper that in order to combat crime the police are seeking the power of tap the phones of anyone they suspect of committing a crime. Do you take this as a serious matter?
1. No concern at all
2. Little concern
3. Very concerned
4. Extremely worried

V40. Do you think it is necessary that this should be controlled or limited by law?
1. Yes
2. No
3. Don't know

V41. Recently, private telephone conversations are being reported publicly in the newspaper to attract readers. Do you take this as a serious matter?
1. No concern at all
2. Little concern
3. Very concerned
4. Extremely worried

V42. Do you think it is necessary that this should be controlled or limited by law?
1. Yes
2. No
3. Don't know

V43. You discover that your Hong Kong tax information is going to be freely available to other departments in the government including Social Welfare Department and Immigration Department. Do you take this as a serious matter?
1. No concern at all
2. Little concern
3. Very concerned
4. Extremely worried

V44. Do you think it is necessary that this should be controlled or limited by law?
1. Yes
2. No
3. Don't know

V45. When you wanted to buy a new television set recently, you asked to pay by cheque. The salesman told you that you could do so, but insisted that you write your I.D. card number on the back of the cheque. Do you take this as a serious matter?
1. No concern at all
2. Little concern
3. Very concerned
4. Extremely worried

V46. Do you think it is necessary that this should be controlled or limited by law?
1. Yes
2. No
3. Don't know

V47. When you wanted to have US$100 changed into Hong Kong dollars in a bank, they asked for your I.D. card number to be recorded. Do you take this as a serious matter?
1. No concern at all
2. Little concern
3. Very concerned
4. Extremely worried

V48. Do you think it is necessary that this should be controlled or limited by law?
1. Yes
2. No
3. Don't know

V49. You have recently run into financial difficulties and are unable to pay your creditors. One day you discover that a debt collecting agency has posted notices in your neighbourhood saying that you owe people money. Do you take this as a serious matter?
1. No concern at all

2. Little concern
3. Very concerned
4. Extremely worried

V50. Do you think it is necessary that this should be controlled or limited by law?
1. Yes
2. No
3. Don't know

With and Without Knowledge Questions

V51. If you applied for a personal loan from a bank and were informed that they would have to check your credit rating with other lending institutions in Hong Kong. Do you take this as a serious matter?
1. No concern at all
2. Little concern
3. Very concerned
4. Extremely worried

V52. Do you think it is necessary that this should be controlled or limited by law?
1. Yes
2. No
3. Don't know

V53. If you applied for a personal loan from a bank and was told that there would be no problem in granting the loan. However, a few days later you discover that the bank, without your knowledge, has checked your credit rating with other lending institutions in Hong Kong. Do you take this as a serious matter?
1. No concern at all
2. Little concern
3. Very concerned
4. Extremely worried

V54. Do you think it is necessary that this should be controlled or limited by law?
1. Yes
2. No
3. Don't know

V55. If you applied for a personal loan from bank and were refused. Do you think you should have the right of access to data which is the basis for the refusal?
1. Yes
2. No

V56. If you believed that the refusal of your bank loan was based on incorrect information, do you think you should have the right of correction of all copies of the incorrect data?
1. Yes
2. No

V57. Do you believe that you should have the right to stop direct mail coming to you?
1. Yes
2. No

V58. Marital Status
1. Single
2. Married
3. Widowed
4. Divorced/Separated
5. No answer

V59. Have you ever been to school? Up to what level?
1. No schooling
2. Primary education (P.1 - P.6)
3. Secondary education (F.1 - F.5)
4. Matriculation (F.6 - F.7)
5. Post-secondary college or above
6. Others
7. No answer

V60. May I know how old you are according to the Western calendar?

V61. How long have you been living in Hong Kong?

**[This is the end of the questionnaire,
thank you for your cooperation.]"**

Appendix 3

Briefing Note for Meeting on Access to Information Bill

Introduction

1. The purpose of this note is to identify some points that may merit discussion at the meeting. It endeavours to identify those aspects of the Bill that could impinge on the Sub-committee's proposals. Those proposals are based on the OECD Guidelines which explicitly attempt to reconcile "fundamental but competing values such as privacy and the free flow of information." Alternative approaches are briefly examined. It does not purport to provide an exhaustive analysis and of course attendees may wish to raise other points.

The intersection of access to information and data protection

A. Access to own data

2. The partial overlap with the Sub-committee's data protection proposals is noted, namely the right to access data about oneself ("data" being the representation of information). Other features of data protection have not been incorporated e.g. transmission of corrections of data to other agencies, limits on the collection of data, use of data to be consistent with original purpose(s), obligations regarding data quality and security. In other words, the Bill does not purport to provide protections regarding the use that is made of the information. In this respect it is narrower than a data protection law ("DPL"). Also, it is limited to the public sector. By the same token, the data protection principles do not address access to data which does not relate to individuals.

B. Access to another's data

3. The Bill, like other FOI laws, provides a qualified right of access to personal data about other individuals. In this respect it is wider than a DPL, which only accords a general right of access to one's own data. Subject to specific exemptions, a DPL, only allows access to third party data when it is relevant to the data user's functions **and** its transfer to that data user is consistent with the purpose for which it is held. These general constraints on access do not apply under the Bill (nor other FOI laws). Similarly, once data has been accessed under the Bill, the data can be deployed for any purpose, whereas under a DPL it must be used consistently with the purpose for which it was obtained.

Exemption for third party data

Clause 21's three tests

5. It follows from the above that the Bill's exemptions to access to third party data are crucial. The following features of cl. 21 accordingly merit discussion:

(i) access to third party data is unrestricted unless it concerns his/her "personal affairs". This expression derives from the 1982 Australian Access to Information Act where it was interpreted as not including, inter alia, occupational performance. The exemption is accordingly significantly narrower than data protection's remit of the regulation of all data relating to an individual. The Australian provision was repealed in 1991 and replaced by a reference to any data about an individual. This brought it into line with their 1989 Privacy Act's definition. Canadian FOI laws also apply their exemption to any data relating to a third party;

(ii) the second limb of the exemption provides that the document contains matter "which it would be unreasonable to disclose";

(iii) the third limb provides that access "would, on balance, be in the public interest".

6. The relationship between (ii) and (iii) is not apparent and clarification is sought.

Does clause 21 sufficiently recognize privacy interests?

7. Also for consideration is whether these tests are sufficiently stringent. For example, the Canadian Access to Information Act requires that the public interest in the disclosure of personal data "**clearly outweighs** any invasion of privacy that could result from disclosure". (The other general ground is that "disclosure would clearly benefit the individual to whom the information relates.") An insufficiently strict test may not conform to the Bill of Rights.

Could clause 21 be more specific?

8. A further aspect is that the Bill does not provide any guidance on how these tests are to be applied. Other clauses in PART IV specify categories of data that are exempt and it is assumed that these would equally apply to third party data. But additional tests as regards personal data merit consideration, to avoid unnecessary uncertainty of application. For example, Canadian FOI laws have detailed supplementary exemptions for personal data to address the special problems they raise. So in determining whether

disclosure would be an unreasonable invasion of a third party's privacy, the 1992 British Columbia Act identifies:

eight relevant factors;

nine situations where such invasion is presumed;

ten situations where disclosure is not unreasonable.

Cross-reference to data protection exemptions

10. As with the enactments of the other Canadian provinces, the legislation encompasses both FOI and data protection. As the Bill envisages that these two matters will be the subject of separate legislation, the approach adopted at the federal level is relevant. As with the Bill, the Canadian Access to Information Act contains various general exemptions from access. As regards personal data, however, the Act provides (s. 19) that access is only authorized if it comes within the relevant provision of the Privacy Act (s. 8). That provision requires that unless the disclosure is consented to, or consistent with the original purpose, it must either fall within one of the narrowly drawn exceptions or the stringent general test mentioned at para. 7 above.

11. The Sub-committee has wrestled with the vexed question of appropriate exemptions along the lines of the Canadian Privacy Act. The Data Protection Ordinance is likely to spell out these exceptions in some detail. A tidy solution, therefore, would be for a provision in the Bill along the lines of the federal Canadian legislation whereby access to third party data is governed by the privacy law. This would enable the two enactments to interlock, reducing their potential for conflict.

Sample Data Purposes return from Australia

Agency: Attorney General's Department

Address: Robert Garran Officers Barton ACT 2600

28 classes of records of personal information are held as follows:

1 Fiscle Computer Package (Financial Records)

The purpose of these records is to pay administrative and legal expenses for all out-rider branches.

Content may include: name, address and goods category.

Sensitive content may include: financial information including debts.

The personal information on these records relates to creditors and debtors.

The following agency staff have access to this personal information: financial staff.

The records are kept 6 years.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting the Certifying Officer, Accounts Section Ph: (062) 719 151.

The records relate to 750 individuals and are stored on computer media.

Location: Corporate Services Branch (Finance Area).

2 Documentation Relating to Federal Offenders

The purpose of these records is to maintain records for administrative and reference purposes. This information is also used for criminal intelligence.

Content may include: name, address, date of birth, occupation, gender, marital status and dependents.

Sensitive content may include: physical or mental health, disabilities, racial or ethnic origin, criminal convictions, criminal intelligence, financial information including debts, relationship details, sentence details and witness protection information in some cases.

The personal information on these records relates to federal offenders.

The following agency staff have access to this personal information: for unclassified material: all staff. For classified material usually: Deputy Secretary, First Assistant Secretary, Senior Assistant Secretary and Principal Legal Officers.

The records are kept for 2 years after expiration of licence/parole or they are destroyed when prisoner reaches or would have reached 99 years of age.

Some of this information is disclosed to: offenders' solicitors (or representatives), relatives, prison and parole authorities and the Australian Federal Police.

Individuals can obtain information regarding access to their personal information by contacting the Principal Legal Officer, Criminal Law and Law Enforcement Division Ph: (062) 719 715.

The records relate to 4 000 individuals and are stored on computer and paper media.

Location: Central Office, Canberra.

3 Documentation Relating to the Remission of Fines or Default Sentences

The purpose of these records is to maintain records for administrative and reference purposes, associated with the exercise of the Royal Prerogative of Mercy.

Content may include: name, address, date of birth, occupation, gender, marital status and dependents.

Sensitive content may include: physical or mental health, disabilities, criminal convictions, tax file numbers, financial information including debts and sentence details.

The personal information on these records relates to federal fine defaulters applying for remissions or pardons.

The following agency staff have access to this personal information: all staff.

The records are kept 5 years.

Some of this information is disclosed to: fine defaulters' accountants, tax agents, solicitors, the Australian Taxation Office and the NSW Attorney-General's Department.

Individuals can obtain information regarding access to their personal information by contacting the FOI Contact Officer Ph: (062) 719 671.

The records relate to 1 300 individuals and are stored on paper media.

Location : Central Office, Canberra.

4 Records on Discrimination in Employment and Occupation

The purpose of these records is to investigate complaints about discrimination in employment. Most complaints investigated fall within categories prescribed in the International Labour Organisation Convention (111) on Discrimination (Employment and Occupation) 1958.

Content may include: name of both complainant and person complained about, address, date of birth, occupation, gender, educational qualifications and physical features (eg. height).

Sensitive content may include: physical or mental health, disabilities, sexual life, racial or ethnic origin, criminal convictions, religious beliefs, political beliefs and relationship details.

The personal information on these records relates to complainants and individuals against whom the complaint is made.

The following agency staff have access to this personal information: staff of the Human Rights and Equal Opportunities Commission and departmental staff whose function it is to appraise records for disposal (AS02-AS06).

The records are kept permanently.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting the FOI Coordinator Ph: (062) 719 519.

The records relate to 1 800 individuals and are stored on paper media.

Location: Central Office, Canberra.

5 Application for Financial Assistance under the Legal Aid Scheme

The purpose of these records is to record information on decisions relating to applications for legal aid or assistance.

Content may include: name, address, date of birth, occupation and gender.

Sensitive content may include: physical or mental health, disabilities, racial or ethnic origin, criminal convictions, financial information including debts, relationship details and legal problem for which legal aid is sought.

The personal information on these records relates to applicants for financial assistance.

The following agency staff have access to this personal information: section officers in the division, officers of the Australian Legal Aid Office and registry officers.

The records are kept 20 years.

Some of this information is disclosed to: external auditors.

Individuals can obtain information regarding access to their personal information by contacting the FOI Coordinator Ph: (062) 719 519.

The records relate to 90 900 individuals and are stored on paper media.

Location : Central Office of Legal Aid Administration.

6 Bankrupt Estates Administration Files

The purpose of these records is to administer estates of insolvent persons for the purposes of the Bankruptcy Act 1966. In addition, these records provide the data from which bankruptcy statistics are collated.

Content may include: name, address, date of birth, occupation, gender, all business transactions (including shareholding, directorships) and, financial and status of those business.

Sensitive content may include: criminal convictions, criminal intelligence, tax file numbers, financial information including debts and relationship details.

The personal information on these records relates to insolvent persons, their creditors, debtors, litigants, family members and associates.

The following agency staff have access to this personal information: all staff.

The records are kept 25 years.

Some of this information is disclosed to: the Australian Taxation Office.

Individuals can obtain information regarding access to their personal information by contacting the Official Receivers in each State or FOI Contact Officers in each State.

The records relate to 90 000 individuals and are stored on computer, paper and sound media.

Location: Central Office Canberra and the Official Receiver in all States.

7 Register of Applications for Custody/Maintenance Orders Abroad

The purpose of these records is to maintain statistics on the number of applications received.

Content may include: name, address, date of birth and gender.

The personal information on these records relates to applicants for registration of orders abroad.

The following agency staff have access to this personal information: staff of the International Section.

The records are kept indefinitely.

Some of this information is disclosed to: persons involved in the registration of maintenance orders.

Individuals can obtain information regarding access to their personal information by contacting the Principal Legal Officer, International Section Ph: (062) 719 368.

The records relate to 1 175 individuals and are stored on paper media.

Location: Canberra Office.

8 Register of Child Abduction Applications

The purpose of these records is to act as agents for parties seeking the return of their child and to maintain statistics on the number of applications received.

Content may include: name, address, date of birth, occupation and gender.

Sensitive content may include: physical or mental health, disabilities, sexual life, racial or ethnic origin, criminal convictions, criminal intelligence, religious beliefs, political beliefs , tax file numbers, financial information including debts and relationship details.

The personal information on these records relates to abducted children, applicants for registration and parents.

The following agency staff have access to this personal information: staff of the International Section.

The records are kept indefinitely.

Some of this information is disclosed to: persons involved in abductions-parents, solicitors, police, courts and foreign government agencies.

Individuals can obtain information regarding access to their personal information by contacting the Principal Legal Officer, International Section Ph: (062) 719 368.

The records relate to 70 individuals and are stored on paper media.

Location: Canberra Office.

9 Quarterly Reports to National Companies and Securities Commission and State Corporate Affairs Offices

The purpose of these records is to record internal and external intelligence under the Companies and Securities Industry Legislation.

Content may include: names of individuals/companies, particulars of alleged offences, status of inquiry and prosecution or result of criminal proceedings.

Sensitive content may include: criminal convictions, criminal intelligence and relationship details.

The personal information on these records relates to persons under investigation.

The following agency staff have access to this personal information: all investigation staff, Commissioner, Deputy Commissioner and Principal Legal Officer.

The records are kept indefinitely.

Some of this information is disclosed to: investigation staff of the National Crimes and Securities Commission, state corporate affairs investigators, the Director of Public Prosecutions, police and the National Crime Authority.

Individuals can obtain information regarding access to their personal information by contacting the Principal Legal Officer Ph: (062) 461 377.

The records relate to 2 000 individuals and are stored on paper media.

Location: Canberra Office.

10 General Files on persons of Interest to Investigations

The purpose of these records is to maintain records of general investigation and intelligence on persons associated with takeovers and company failures.

Content may include: name, address, date of birth, occupation and gender.

Sensitive content may include: racial or ethnic origin, criminal convictions, criminal intelligence, financial information including debts and relationship details.

The personal information on these records relates to persons under investigation.

The following agency staff have access to this personal information: all investigation staff, Commissioner, Deputy Commissioner and Principal Legal Officer.

The records are kept indefinitely.

Some of this information is disclosed to: the Director of Public Prosecutions, the police and the National Crime Authority.

Individuals can obtain information regarding access to their personal information by contacting the Principal Legal Officer Ph: (062) 461 377.

The records relate to 160 individuals and are stored on computer and paper media.

Location: Canberra Office.

11 Files on Registered Company Auditors and Liquidators

The purpose of these records is to record the registration of liquidators and conditions as required by Division 2 of Part 2 of the Companies Act 1981.

Content may include: name, address, date of birth, employment history, places of residence and personal references.

Sensitive content may include: criminal convictions.

The personal information on these records relates to registered liquidators, auditors and applicants.

The following agency staff have access to this personal information: all staff in the Corporate Finance and Accounting Section, Commissioner, Deputy Commissioner and Principal Legal Officer.

The records are kept permanently.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting the Corporate Affairs Commission ACT Ph: (062) 461 340.

The records relate to 160 individuals and are stored on paper media.

Location: Canberra Office.

12 Licencees under Securities Industries Act and Futures Industry Act

The purpose of these records is to licence dealers and advisers under the conditions prescribed by the Securities Industry Act.

Content may include: name, address, date of birth, employment history, places of residence and personal references.

Sensitive content may include: criminal convictions.

The personal information on these records relates to licensed advisers and dealers.

The following agency staff have access to this personal information: all staff in the Corporate Finance and Accounting Section, Commissioner, Deputy Commissioner and Principal Legal Officer.

The records are kept indefinitely.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting the ACT Corporate Affairs Commission Ph: (062) 461 340.

The records relate to 585 individuals and are stored on paper media.

Location: Canberra Office.

13 Major Case Management and Investigation Files

The purpose of these records is to maintain investigation records and evidence obtained regarding alleged offences against the Companies and Securities Legislation.

Content may include: name, address, date of birth and occupation.

Sensitive content may include: racial or ethnic origin, criminal convictions, criminal intelligence, financial information including debts, relationship details and bankruptcy details.

The personal information on these records relates to alleged offenders.

The following agency staff have access to this personal information: all investigation staff, Commissioner, Deputy Commissioner and Principal Legal Officer.

The records are kept indefinitely.

Some of this information is disclosed to: the Director of Public Prosecutions, the police and the National Crime Authority.

Individuals can obtain information regarding access to their personal information by contacting the Principal Legal Officer Ph: (062) 461 377.

The records relate to 2 300 individuals and are stored on computer, paper and sound media.

Location: Canberra Office.

14 Register of Proceedings/ Informations Laid/Sworn Alleged Offenders

The purpose of these records is to assist with investigation and intelligence gathering related to the Securities Industry Legislation.

Content may include: name, address and particulars of alleged offence.

Sensitive content may include: details of alleged offences.

The personal information on these records relates to alleged offenders.

The following agency staff have access to this personal information: all investigations staff, Commissioner, Deputy Commissioner and Principal Legal Officer.

The records are kept indefinitely.

Some of this information is disclosed to: the Director of Public Prosecution, the police and the National Crime Authority.

Individuals can obtain information regarding access to their personal information by contacting the Principal Legal Officer Ph. (062) 461 377.

The records relate to 60 individuals and are stored on paper media.

Location: Canberra Office.

15 Register of Convicted Persons

The purpose of these records is to assist internal reporting and intelligence gathering under the Companies and Securities Legislation.

Content may include: name, relevant company details and details of offences.

Sensitive content may include: criminal convictions, criminal intelligence and relationship details.

The personal information on these records relates to alleged offenders.

The following agency staff have access to this personal information: all investigation staff, Commissioner and Deputy Commissioner.

The records are kept indefinitely.

Some of this information is disclosed to: the Director of Public Prosecutions, the police, other law enforcement agencies and the National Crime Authority.

Individuals can obtain information regarding access to their personal information by contacting the Principal Legal Officer Ph: (062) 461 3777.

The records relate to 400 individuals and are stored on paper media.

Location: Canberra Office.

16 Extradition, Mutual Assistance in Criminal Matters and Status of Forces Case Files

The purpose of these records is to secure extradition from or to Australia or to get evidence for criminal trials in Australia or overseas or for the purpose of waiver of jurisdiction issues under the Defence (Visiting Forces) Act.

Content may include: name, address, occupation (if relevant), date of birth, gender, fingerprints (if relevant), citizenship, description (if relevant) and associates (if relevant).

Sensitive content may include: physical or mental health, disabilities, racial or ethnic origin, criminal convictions, criminal intelligence, political beliefs, financial information including debts and relationship details.

The personal information on these records relates to fugitives from justice and witnesses for criminal prosecutions.

The following agency staff have access to this personal information: all officers of the International Branch, staff of the Criminal Law and Law Enforcement Division and registry staff.

The records are kept permanently.

Some of this information is disclosed to: law enforcement agencies in and outside of Australia (eg. the Australian Federal Police, Interpol, National Crime Authority, Australian Security Intelligence Organisation), Courts and Prosecutors in and out of Australia, the Department of Foreign Affairs, Australian Missions Abroad and Foreign Embassies in Australia.

Individuals can obtain information regarding access to their personal information by contacting the FOI Contact Officer Ph: (062) 719 111.

The records relate to 157 individuals and are stored on paper and pictorial media.

Location: Central Office, Canberra.

17 Royal Commission into Aboriginal Deaths in Custody

The purpose of these records is to maintain unreleased reports of the Royal Commission into Aboriginal Deaths in custody.

Content may include: conduct, name, address, date of birth, occupation and gender.

Sensitive content may include: allegations of criminal and improper or negligent conduct.

The personal information on these records relates to persons involved in the investigation of deaths.

The following agency staff have access to this personal information: Principal Adviser and Commission Secretariat.

The records are kept permanently for policy matters, or 10 years for other information.

Some of this information is disclosed to: the public by tabling in Parliament.

Individuals can obtain information regarding access to their personal information by contacting the Principal Adviser, Aboriginal Death Secretariat Ph: (062) 719 860.

The records relate to 300 individuals and are stored on paper media.

Location: Central Office, Canberra.

18 Applications for Appointment as Marriage Celebrants (Civil and Religious)

The purpose of these records is to appoint and record authorised Civil and Religious Celebrants, Civil Marriage Applicants, and to maintain statistics.

Content may include: name, address, authorization number, church, date of authorization, phone number, yearly statistics, electoral name, file number, location (town and city).

The personal information on these records relates to members of the public, registrar officers and ministers of religion (defined by the Marriage Act).

The following agency staff have access to this personal information: Marriage Celebrants Section Staff.

The records are kept permanently for prominent persons. Information on appointed celebrants are kept until the celebrant reaches 99 years of age or 2 years after death.

Some of this information is disclosed to: the general public, Registrars of Birth, Deaths and Marriages and to Ministers of Religion.

Individuals can obtain information regarding access to their personal information by contacting the Family Law Branch Ph: (062) 719 848.

The records relate to 16 000 individuals and are stored on paper media.

Location: Central Office, Canberra.

19 Determination of Refugee Status Committee-Applications

The purpose of these records is to enable consideration and determination of claims for refugee status.

Content may include: name, address, date of birth, family, occupation, gender, race and biography.

Sensitive content may include: physical or mental health, racial or ethnic origin, criminal convictions, religious beliefs, political beliefs and relationship details.

The personal information on these records relates to prohibited immigrants and applicants for refugee status.

The following agency staff have access to this personal information: Freedom of Information Officers and Human Rights Branch staff.

The records are kept for up to 4 years after last action.

Some of this information is disclosed to: persons representing departments or bodies on the Determination of Refugee Status (DORS) Committee, the Department of Immigration, Local Government and Ethnic Affairs, the Department of Foreign Affairs and Trade, the Department of Prime Minister and Cabinet and the United Nations High Commissioner of Refugees.

Individuals can obtain information regarding access to their personal information by contacting the FOI Contact Officer Ph: (062) 719 111.

The records relate to 3 000 individuals and are stored on paper media.

Location: Central Office, Canberra.

20 Biographical/Personal Information on Judges and Tribunal Members

The purpose of these records is to advise Cabinet/Executive Council upon appointment/reappointment of judges and tribunal members and advise on applicable terms and conditions of service.

Content may include: name, address, date of birth, employment history, qualifications and number of children.

Sensitive content may include: relationship details.

The personal information on these records relates to judges and tribunal members.

The following agency staff have access to this personal information: officers of the Courts and Tribunals Branch.

The records are kept permanently.

Some of this information is disclosed to: Cabinet and Executive Council.

Individuals can obtain information regarding access to their personal information by contacting the Senior Assistant Secretary, Courts and Tribunal Branch Ph: (062) 719 240.

The records relate to 200 individuals and are stored on computer and paper media.

Location: Canberra, Central Office.

21 Central Index

The purpose of these records is to control records and to assist with the identification and retrieval of files.

Content may include: name and occupation.

Sensitive content may include: criminal convictions and relationship details.

The personal information on these records relates to employees and members of the public.

The following agency staff have access to this personal information: registry staff and some departmental action officers have access to file titles.

The records are kept permanently.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting the FOI Co-ordinator Ph: (062) 719 519.

The records relate to 50 000 individuals and are stored on computer, paper and microfiche media.

Location: Central office, Canberra.

22 Declaration of Pecuniary Interests

The purpose of these records is to register interests of Senior Public Servants required by Public Services Board Joint Council memoranda of 27 July 1984 and 3 September 1984.

Content may include: name and address.

Sensitive content may include: financial information including debts and relationship details.

The personal information on these records relates to Ministers, senior public servants, ministerial staff and senior staff of statutory authorities.

The following agency staff have access to this personal information: Ministers in the case of Statutory Office Holders and Heads of Agencies and Heads of Agencies in the case of Senior Public Servants.

The records are kept indefinitely.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting the Attorney General's office Ph: (062) 777 730 (for statutory authority heads) Secretary Ph: (062) 719 000 (for senior public servants).

The records relate to an unknown number of individuals and are stored on paper media.

Location: Central Office, Canberra (for senior public servants) and Attorney General's Office, Parliament House (for State Office Heads).

23 Personal Information on Commissioners for Declarations

The purpose of these records is to keep track of persons appointed as Commissioners in order to contact them if necessary.

Content may include: name and address (private and business).

Sensitive content may include: relationship details.

The personal information on these records relates to Commonwealth public servants and members of the public.

The following agency staff have access to this personal information: officers of the Courts and Tribunals Branch.

The records are kept until the person's commission is revoked.

Some of this information is disclosed to : the organisations employing the person appointed as Commissioners for Declarations.

Individuals can obtain information regarding access to their personal information by contacting the Director, Resources, Terms and Conditions Section, Courts and Tribunals Branch, Ph: (062) 719 106.

The records relate to 5 000 individuals and are stored on computer and paper media.

Location: Canberra, Central Office.

24 Police Checks on Applicants External to the Commonwealth Public Services

The purpose of these records is to ascertain if an applicant is a fit and proper person to be appointed as a Commissioner for Declarations.

Content may include: name, address, place of birth and date of birth.

Sensitive content may include: criminal convictions.

The personal information on these records relates to members of the public.

The following agency staff have access to this personal information: officers of the Courts and Tribunals Branch.

The records are kept 7 years.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting the Director Resources, Terms and Conditions Section, Courts and Tribunals Branch, Ph: (062) 719 106.

The records relate to 1 000 individuals and are stored on paper media.

Location: Canberra, Central Office.

25 Appointments to the Administrative Review Council (ARC)

The purpose of these records is to advise the Attorney-General on appointments and re-appointments to the Administrative Review Council.

Content may include: name, address, date of birth, occupation, gender, curriculum vitae, work history, professional and educational qualifications.

Sensitive content may include: racial or ethnic origin and relationship details.

The personal information on these records relates to members and potential members of the Australian Review Council.

The following agency staff have access to this personal information: personnel in the Administrative Law and Legal Procedures Branch.

The records are kept permanently.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting

the Principal Legal Officer, Administrative Law and Legal Procedures Branch Ph: (062) 719 354.

The records relate to an unknown number of individuals and are stored on paper media.

Location: Attorney-General's Department, Canberra, ACT.

26 Student Records of Australian Police Staff College

The purpose of these records is to maintain student records which contain work histories, personal and family details and records of attendance at particular courses.

Content may include: name, address, date of birth, occupation, gender, work history, family details and record of attendance for courses.

Sensitive content may include: relationship details and professional biography.

The personal information on these records relates to students.

The following agency staff have access to this personal information: Director/Dean of Studies and Director of Programs.

The records are kept indefinitely.

Some of this information is disclosed to: the Commissioner of Police.

Individuals can obtain information regarding access to their personal information by contacting the Director/ Dean of Students Australian Police Staff College Ph: (02) 977 5800.

The records relate to 2 500 individuals and are stored on paper media.

Location: Australian Police Staff College.

27 Statutory Authorities Senior Appointments System

The purpose of these records is to inform department senior officers and portfolio Ministers, when appointments expire. It also provides Ministers with an up to date list of all appointees.

Content may include: name, address, date of birth, occupation, gender, appointment held and curriculum vitae.

The personal information on these records relates to employees.

The following agency staff have access to this personal information: 4 designated staff in the Ministerial and Parliamentary Section and 5 designated staff in the Courts and Tribunals Branch.

The records are kept indefinitely.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting the Parliamentary Liason Section Ph: (062) 719 592.

The records relate to an unknown number of individuals and are stored on computer media.

Location : Parliamentary Section, Courts and Tribunals Branch.

28 Personnel/Staff Records

The purpose of these records is to record employment details of staff for the following work related matters: recruitment, promotion, career development, studies assistance, security, compensation, leave, salary, attendance, grievances and general personnel matters.

Content may include: name, address, date of birth, occupation, appointments held, time in position, development options, job training, service employment history, accident details, bank account numbers and superannuation.

Sensitive content may include: physical or mental health, disabilities, sexual life, racial or ethnic origin, criminal convictions, tax file numbers, financial information including debts, relationship details, salary history, discipline and counselling records.

The personal information on these records relates to employees.

The following agency staff have access to this personal information: Career Development Officer, Inspector Career Development, Management, Staff Development Officer, Personnel Section staff, Directors, Studies Assistance Officer, Staff Clerk and Assistant Director Corporate Services.

The records are kept permanently for SES Officers or until the employee attains 67 years of age, or 1-7 years depending on the nature of the record.

Some of this information is disclosed to: Comcare, rehabilitation providers, treating medical practioners, other Commonwealth agencies on transfer or promotion and the Public Service Commission.

Individuals can obtain information regarding access to their personal information by contacting the Career Development Officer Ph: (062) 719 142 or Staff Development Officer Ph: (062) 719 188 or Assistant Director of Staffing Ph: (062) 719 117 or Personnel Officer Ph: (062) 719 125 or the Personnel Officer in State Branches.

The records relate to an unknown number of individuals and are stored on computer, paper and microfiche media.

Location: Central Office and State Offices.

152 Statements - Witness and Crime Scene

The purpose of these records is to record details of crime scene.

Content may include: name, address, date of birth, occupation and phone number.

Sensitive content may include: physical or mental health, disabilities, sexual life, racial or ethnic origin, criminal convictions, criminal intelligence, religious beliefs, political beliefs, tax file numbers, financial information including debts and relationship details.

The personal information on these records relates to police, offenders, complainants and witnesses.

The following agency staff have access to this personal information: staff in all operational areas.

The records are kept for up to 10 years after final action.

Some of this information is disclosed to: courts.

Individuals can obtain information regarding access to their personal information by contacting the Australian Federal Police Administrative Law Branch Canberra Ph: (062) 757 210.

The records relate to 10 000 individuals and are stored on paper media.

Location: Scientific Branch, Weston ACT.

153 State Police Alerts

The purpose of these records is to assist in police investigations.

Content may include: name, address and date of birth.

Sensitive content may include: criminal convictions, criminal intelligence and relationship details.

The personal information on these records relates to offenders and suspects.

The following agency staff have access to this personal information: members of Portswatch Section.

The records are kept indefinitely.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting the Australian Federal Police Administrative Law Branch Canberra Ph: (062) 757 210.

The records relate to 100 000 individuals and are stored on paper media.

Location: Portswatch Section in Regional Offices.

154 State Police Computer Index

The purpose of these records is to provide a reference source for conducting investigations.

Content may include: name, date of birth, address, occupation and gender.

Sensitive content may include: criminal convictions and criminal intelligence.

The personal information on these records relates to persons of interest to the police.

The following agency staff have access to this personal information: members of Intelligence Division in Regional Offices.

The records are kept permanently.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting the Australian Federal Police Administrative Law Branch Canberra Ph: (062) 757 210.

The records relate to an unknown number of individuals and are stored on computer media.

Location: AFP computer terminals.

155 Stolen Motor Vehicle Register

The purpose of these records is to record stolen motor vehicle particulars.

Content may include: name, address, date of birth and occupation.

Sensitive content may include: criminal convictions and criminal intelligence.

The personal information on these records relates to complainants, witnesses, offenders and police.

The following agency staff have access to this personal information: staff in all areas of the AFP.

The records are kept indefinitely.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting the Australian Federal Police Administrative Law Branch Canberra Ph: (062) 757 210.

The records relate to 70 000 individuals and are stored on paper media.

Location: Information (Crime) Branch.

156 Stolen Property Report

The purpose of these records is to record stolen property.

Content may include: name, address, date of birth, occupation and details of property stolen.

Sensitive content may include: criminal convictions and criminal intelligence.

The personal information on these records relates to complainants, offenders and police.

The following agency staff have access to this personal information: staff in all areas of the AFP.

The records are kept for up to 10 years after action ceases.

Some of this information is disclosed to: courts and insurance companies.

Individuals can obtain information regarding access to their personal information by contacting the Australian Federal Police Administrative Law Branch Canberra Ph: (062) 757 210.

The records relate to 100 000 individuals and are stored on paper media.

Location: Information (Crime) Branch.

157 Summons – Application and Information

The purpose of these records is to apply to courts for summons.

Content may include: name, address, date of birth, occupation and alleged offence.

Sensitive content may include: criminal convictions and criminal intelligence.

The personal information on these records relates to police and offenders.

The following agency staff have access to this personal information: staff in all areas of the AFP.

The records are kept for up to 10 years after final action.

Some of this information is disclosed to: courts, the Director of Public Prosecutions, solicitors and the Australian Government Solicitor.

Individuals can obtain information regarding access to their personal information by contacting the Australian Federal Police Administrative Law Branch Canberra Ph: (062) 757 210.

The records relate to 100 000 individuals and are stored on paper media.

Location: Legal Services Division.

158 Sundry Debtors and Register Advice

The purpose of these records is to record debt and request payment.

Content may include: name and address.

Sensitive content may include: financial information including debts.

The personal information on these records relates to persons concerned with debt.

The following agency staff have access to this personal information: the Receiver of Public Monies.

The records are kept for up to 3 years after final action.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting the Australian Federal Police Administrative Law Branch Canberra Ph: (062) 757 210.

The records relate to 30 000 individuals and are stored on computer and paper media.

Location: Receiver of Public Monies, ACT and Regions.

159 Surveillance Log Sheets

The purpose of these records is to assist in investigations.

Content may include: name, address, date of birth, gender, occupation, records of time and places and vehicle movements.

Sensitive content may include: criminal intelligence and relationship details.

The personal information on these records relates to persons under investigation.

The following agency staff have access to this personal information: members of Organised Crime Branch and other authorised AFP members.

The records are kept for up to 3 years after final action.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting the Australian Federal Police Administrative Law Branch Canberra Ph: (062) 757 210.

The records relate to 200 000 individuals and are stored on computer and paper media.

Location: Organised Crime Branch in Regional Offices.

160 Tasking Form

The purpose of these records is to record requests for Police Technical Unit assistance.

Content may include: name, address, date of birth and occupation.

Sensitive content may include : physical or mental health, disabilities, sexual life, racial or ethnic origin,

Agency: Department of Prime Minister and Cabinet

Address: 3-5 National Circuit Barton ACT 2600

16 classes of records of personal information are held as follows :

1 Correspondence to Prime Minister

The purpose of these records is to maintain a record of correspondence received by and answered by the Prime Minister and his Department.

Content may include: name, address and any other information volunteered by the correspondent.

Sensitive content may include: physical or mental health, disabilities, sexual life, racial or ethnic origin, criminal convictions, criminal intelligence, religious beliefs, political beliefs, tax file numbers, financial information including debts and relationship details.

The personal information on these records relates to any individual who chooses to write to the Prime Minister.

The following agency staff have access to this personal information: staff who are processing or preparing a response to the correspondence.

The records are kept for at least 1 year, or permanently for policy matters.

Some of this information is disclosed to: other departments if they are involved in the preparation of the response.

Individuals can obtain information regarding access to their personal information by contacting the Privacy Contact Officer Ph: (062) 715 769.

The records relate to 55 000 individuals and are stored on computer, paper and sound media.

Location: 3-5 National Circuit Barton ACT.

2 Executive Council Appointments Documents

The purpose of these records is to meet the requirements of the Executive Council and produce minutes for meetings.

Content may include: name, address, date of birth, employment history and membership of organisations.

The personal information on these records relates to potential and confirmed appointees to statutory positions.

The following agency staff have access to this personal information: staff in the Executive Council Secretariat .

The records are kept permanently.

Some of this information is disclosed to: the public by way of ministerial announcements (this information is not usually disclosed by the department).

Individuals can obtain information regarding access to their personal information by contacting the Privacy Contact Officer Ph: (062) 715 769.

The records relate to approximately 100 individuals and are stored on paper media.

Location: 3-5 National Circuit, Barton ACT.

3 Records of High-Level Official Visitors

The purpose of these records is to maintain a record of visit to allow adequate planning of the visit.

Content may include: name, portfolio, Australian itinerary, programme and dietary restrictions.

Sensitive content may include: physical or mental health, racial or ethnic origin, religious beliefs and political beliefs.

The personal information on these records relates to official overseas visitors.

The following agency staff have access to this personal information: all members of ceremonial and hospitality branch.

The records are kept permanently.

Some of this information is disclosed to: officers of cooperating Commonwealth and State Government Departments working on each official visit.

Individuals can obtain information regarding access to their personal information by contacting the Privacy Contact Officer Ph: (062) 715 769.

The records relate to 3 000 individuals and are stored on computer, paper and pictorial media.

Location: 3-5 National Circuit, Barton ACT.

4 Royal Commission Records

The purpose of these records is to maintain a record of Royal Commissions for administrative and historical purposes.

Content may include: information pertinent to the particular Royal Commission including name.

Sensitive content may include: physical or mental health, disabilities, racial or ethnic origin, criminal convictions, criminal intelligence, religious beliefs, political beliefs, financial information including debts and relationship details.

The personal information on these records relates to participants or those involved in or subject of a particular Royal Commission.

The following agency staff have access to this personal information: officers in the Government and Legal Branch and records management staff.

The records are kept permanently.

Some of this information is disclosed to: agencies or individuals who provided the requested information to the Commission. Some information may be disclosed to law enforcement agencies (if it is not confidential).

Individuals can obtain information regarding access to their personal information by contacting the Privacy Contact Officer Ph: (062) 715 769.

The records relate to individuals and are stored on computer and paper media.

Location: Australian Archives Offices in the capital cities where the Commission was held and 3-5 National Circuit, Barton ACT.

5 Cabinet Appointments System

The purpose of these records is to record Cabinet appointments to government organisations, statutory bodies a

Content may include: name, address, date of birth, gender, occupation, membership of government and other bodies and non-English speaking and background.

Sensitive content may include: financial information.

The personal information on these records relates to any person considered for appointment by the Cabinet.

The following agency staff have access to this personal information: cabinet office staff and staff in the relevant branches who are preparing cabinet briefings on the appointments.

The records are kept permanently.

Some of this information is disclosed to: originating/relevant portfolio areas for updating purposes.

Individuals can obtain information regarding access to their personal information by contacting the Cabinet Office Ph: (062) 715 321.

The records relate to 1 100 individuals and are stored on computer and paper media.

Location: Cabinet Office, 3-5 National Circuit, Barton ACT.

6 Table of Precedence Details

The purpose of these records is to maintain a record for guest list purposes for official occasions, ceremonies of State and for notification purposes in the event of State funerals.

Content may include: name, title, address, position, post nominals, marital status, spouse/partner and phone number.

Sensitive content may include: relationship details.

The personal information on these records relates to executive, judiciary, Parliamentary officials, diplomatic officials, defence officials, ecclesiastic officials, state and local government officials and senior public officials.

The following agency staff have access to this personal information: all officers of the Ceremonial and Hospitality branch.

The records are kept until updated.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting the Privacy Contact Officer Ph: (062) 715 769.

The records relate to 1 070 individuals and are stored on computer and paper media.

Location: 3-5 National Circuit, Barton, ACT.

7 Intelligence and Security Records

The purpose of these records is to facilitate coordination and preparation of briefings for the Prime Minister, on matters of intelligence and security.

Content may include: name (it should be noted that the intelligence and security records are not nominal records: they are topic related. The majority of documents they contain originate from one or more of the intelligence agencies or other exempt agencies and would therefore be exempt from the operation of the Privacy Act 1988).

Sensitive content may include: racial or ethnic origin, criminal convictions, criminal intelligence, religious beliefs and political beliefs.

The personal information on these records relates to individuals who may have a bearing on matters of national security.

The following agency staff have access to this personal information: staff in the Office of Security and Intelligence Coordination, Division Head, Deputy Secretary and Secretary.

The records are kept permanently.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting the Privacy Contact Officer Ph: (062) 715 769.

The records relate to individuals and are stored on paper media.

Location: 3-5 National Circuit, Barton ACT.

8 Documents Relating to Awards

The purpose of these records is to seek the Prime Minister's support for, or recommendation of, awards in the Order of Australia and to seek the Governer-General's permission on the acceptance of a foreign honour.

Content may include: name, address, date of birth, occupation, previous awards history and activities undertaken relating to award.

The personal information on these records relates to Australians and citizens of other countries.

The following agency staff have access to this personal information: Ceremonial and Hospitality Branch staff (AS06), Director, Assistant Secretary, First Assistant Secretary, Deputy Secretary and Secretary.

The records are kept permanently.

Some of this information is disclosed to: Government House, Prime Minister's Office and the Department of Administrative Services - Awards and National Symbols Branch.

Individuals can obtain information regarding access to their personal information by contacting the Privacy Contact Officer Ph: (062) 715 769.

The records relate to about 350 individuals and are stored on paper media.

Location: 3-5 National Circuit, Barton ACT.

9 Documents Relating to Applications for Consultancies

The purpose of these records is to record applications for consultancies and selection procedures.

Content may include: name, address, date of birth, occupation, curriculum vitae and referees reports.

Sensitive content may include: financial information including debts.

The personal information on these records relates to potential consultants.

The following agency staff have access to this personal information: staff engaging consultants.

The records are kept 1 to 5 years.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting the Privacy Contact Officer Ph: (062) 715 769.

The records relate to 400 individuals and are stored on paper media.

Location: 3-5 National Circuit, Barton ACT.

10 Documents Relating to Grant Applications

The purpose of these records is to select, process and record applications for grants.

Content may include: name, address and position in relevant organisations.

The personal information on these records relates to grant applicants and recipients.

The following agency staff have access to this personal information: staff in relevant area (eg office of the Status of Women and Office of Multicultural Affairs).

The records are kept for operational current use.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting the Privacy Contact Officer Ph: (062) 715 769.

The records relate to 1 000 individuals and are stored on computer and paper media.

Location: 3-5 National Circuit, Barton ACT.

11 Register of Women

The purpose of these records is to provide a source of names for possible appointment to Commonwealth boards, authorities and instrumentalities.

Content may include: name, address, date of birth, educational qualifications, occupation, interests/expertise, employment history, appointments - Commonwealth/State, membership of organisations and EEO status.

Sensitive content may include: disabilities and racial or ethnic origin.

The personal information on these records relates to women.

The following agency staff have access to this personal information: all staff in the Office of the Status of Women.

The records are kept until updated.

Some of this information is disclosed to: Commonwealth Departments and Commonwealth Ministers offices on request.

Individuals can obtain information regarding access to their personal information by contacting the Privacy Contact Officer Ph: (062) 715 769.

The records relate to 900 individuals and are stored on computer and paper media.

Location: Office of Status of Women, 3-5 National Circuit, Barton, ACT, 2600.

12 Information on Determination of Refugee Status

The purpose of these records is to prepare replies to correspondence and assessment of applications for refugee status.

Content may include: name, address, nationality, occupation and family membership.

Sensitive content may include: racial or ethnic origin, religious beliefs, political beliefs and relationship details.

The personal information on these records relates to applicants for Australian resident status.

The following agency staff have access to this personal information: officers in the International Division.

The records are kept 5 years or permanently for policy or precedent reasons.

Some of this information is disclosed to: the Department of Immigration Local Government and Ethnic Affairs.

Individuals can obtain information regarding access to their personal information by contacting the Privacy Contact Officer Ph: (062) 715 769.

The records relate to 2 000 individuals and are stored on paper media.

Location: 3-5 National Circuit, Barton ACT.

13 Statements of Private Interests by SES Officers

The purpose of these records is to place on record interests of staff which may conflict or may be seen to conflict with their public duty.

Content may include: name and address.

Sensitive content may include: financial

information including debts.

The personal information on these records relates to SES officers.

The following agency staff have access to this personal information: Secretary of the Department.

The records are kept 1 year.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting the Executive Assistant Ph: (062) 715 208.

The records relate to 32 individuals and are stored on paper media.

Location: 3-5 National Circuit, Barton ACT.

14 Personal Security File

The purpose of these records is to conduct a security assessment of employees in relation to suitability for access to national security and/or national interest classified matter and/or entry to a secure area.

Content may include: name, address, date/place of birth, occupation, gender, spouse, parents, overseas travel, education, interview records and nationality.

Sensitive content may include: sexual life, racial or ethnic origin, criminal convictions, religious beliefs, political beliefs, financial information including debts and relationship details.

The personal information on these records relates to employees and contractors who require access to classified matter or secure areas.

The following agency staff have access to this personal information: Security Officer, Assessments Officer, Assistant Security Officer, First Assistant Secretary Corporate Services Division and Director Departmental Security.

The records are kept 1 year after retirement/resignation.

Some of this information is disclosed to: other Commonwealth agencies on transfer and promotion to a designated security assessment position.

Individuals can obtain information regarding access to their personal information by contacting the Departmental Security Section Ph: (062) 715 153.

The records relate to 1 200 individuals and are stored on paper and pictorial media.

Location: Departmental Security Section, 3-5 National Circuit, Barton ACT.

15 Appointments Approved by the Prime Minister

The purpose of these records is to maintain a record of appointments which are approved by the Prime Minister and which do not require Cabinet or Executive Council consideration.

Content may include: name, address, date of birth, employment history and membership of organisations.

The personal information on these records relates to potential and confirmed appointees to government advisory bodies.

The following agency staff have access to this personal information: staff in the relevant branches who are preparing briefings and correspondence on the appointments.

The records are kept permanently.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting the Privacy Contact Officer Ph: (062) 715 769.

The records relate to 30 individuals and are stored on computer and paper media.

Location: 3-5 National Circuit, Barton, ACT, 2600

16 Personnel Files

The purpose of these records is to assist with the efficient operation of the personnel subsection, maintaining work related records of employment history and recruitment, salary, compensation and discipline matters.

Content may include: name, address, date of birth, occupation, gender, career history, applications for positions, interview and referee records, qualifications and allowances.

Sensitive content may include: physical or mental health, disabilities and tax file numbers.

The personal information on these records relates to employees of the department.

The following agency staff have access to this personal information: all staff in personnel sub-section and selection staff.

The records are kept permanently for SES Officers, or until the employee reaches 75 years of age.

Some of this information is disclosed to : other government departments on transfer or promotion.

Individuals can obtain information regarding access to their personal information by contacting the Privacy Contact Officer Ph: (062) 715 769.

The records relate to 1 000 individuals and are stored on computer and paper media.

Location: 3-5 National Circuit, Barton ACT.

Agency: Commonwealth Ombudsman

Address: GPO Box 442 Canberra ACT 2601

5 classes of records of personal information are held as follows:

1 File Register

The purpose of these records is to maintain a manual record of all files made up for the investigation of complaints in the period 1977-1985.

Content may include: name, complaint, file number, address and nature of complaint.

Sensitive content may include: physical and mental health, disabilities, sexual life, racial or ethnic origin, criminal convictions, criminal intelligence, religious beliefs, political beliefs, tax file numbers, financial information including debts and relationship details.

The personal information on these records relates to complainants.

The following agency staff have access to this personal information: all staff.

The records are kept indefinitely, until disposal authorities are created.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting the Publicity and Information Officer Ph: (062) 760 145.

The records relate to 17 000 individuals and are stored on paper media.

Location: Canberra Central Office.

2 Name Index Cards

The purpose of these records is to enable access to correspondence (ie complaints files) for purpose of the investigation of complaints.

Content may include: name, correspondence and file number(s).

Sensitive content may include: physical or mental health, disabilities, sexual life, racial or ethnic origin, criminal convictions, criminal intelligence, religious beliefs, political beliefs, tax file numbers, financial information including debts and relationship details.

The personal information on these records relates to complaints (ie. any person affected by Commonwealth government or ACT administration).

The following agency staff have access to this personal information: all staff.

The records are kept until complaints are finalised and then indefinitely pending on creation of disposal authorities.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting the Publicity and Information Officer Ph: (062) 760 145.

The records relate to 25 000 individuals and are stored on paper media.

Location: Central Office, Canberra.

3 Correspondence Flies (Complaints)

The purpose of these records is to assist the investigation of complaints under the Ombudsman Act 1976, Complaints (Australian Federal Police) Act 1981, FOI Act 1982 and ACT Ombudsman Ordinance 1989.

Content may include: name, address, gender and nature of complaint.

Sensitive content may include: physical or mental health, disabilities, sexual life, racial or ethnic origin, criminal convictions, criminal intelligence, religious beliefs, political beliefs, tax file numbers, financial information including debts and relationship details.

The personal information on these records relates to complainants (ie. any person affected by Commonwealth government or ACT administration).

The following agency staff have access to this personal information: all staff can access general complaints files. Police complaints files are classified and allocated on a need to know basis.

The records are kept until finalisation of complaint. In more complex cases, until any appeal has been finalised and to allow for requests under the FOI act.

Some of this information is disclosed to: the relevant Commonwealth agency that is the subject of complaint.

Individuals can obtain information regarding access to their personal information by contacting the Investigation Officer handling the complaint, Ph: (062) 760 111.

The records relate to 25 000 individuals and are stored on computer, paper and sound media.

Location: Central Office, Canberra and Offices in all State Capitals.

4 Administration Files (Policy)

The purpose of these records is to carry out the functions of the Ombudsman's Office.

Content may include: name, address, gender, occupation and date of birth.

Sensitive content may include: physical or mental health, disabilities, sexual life, racial or ethnic origin, criminal convictions, criminal intelligence, political beliefs, tax file numbers, financial information including debts and relationship details.

The personal information on these records relates to complainants and employees.

The following agency staff have access to this personal information: all staff.

The records are kept indefinitely until disposal authorities are created.

Some of this information is disclosed to: the Department of Prime Minister and Cabinet.

Individuals can obtain information regarding access to their personal information by contacting the FOI Officer Ph: (062) 760 145.

The records relate to 3 000 individuals and are stored on computer and paper media.

Location: Central Office, Canberra.

5 Personnel Files

The purpose of these records is to record details of employees of the Ombudsman's Office.

Content may include: name, address, date of birth, occupation, gender, salary, referee reports, tax file numbers, financial information including debts and relationship details.

Sensitive content may include: physical or mental health, disabilities, sexual life, racial or ethnic origin, criminal convictions, criminal intelligence, religious beliefs, political beliefs, tax file numbers, financial information including debts and relationship details.

The personal information on these records relates to employees.

The following agency staff have access to this personal information: Ombudsman, Deputy Ombudsman, Central Administration staff, SES Administration, Officer in Charge of Personnel, Executive Officer, Personnel and Recruitment Officer.

The records are kept until employment ceases then indefinitely pending creation of disposal authorities.

Some of this information is disclosed to: the Department of Prime Minister and Cabinet.

Individuals can obtain information regarding access to their personal information by contacting the Personnel and Recruitment Officer Ph: (062) 760 139.

The records relate to 70 individuals and are stored on computer and paper media.

Location: Central Office, Prudential Building, Corner University Avenue/ London Circuit, Canberra.

Agency: Merit Protection and Review Agency

Address: 65-67 Constitution Avenue Campbell ACT 2601

4 classes of records of personal information are held as follows:

1 Review Committees Program

The purpose of these records is to enable review committees constituted pursuant to the Merit Protection (Australian Government Employees) Act to determine appeals and applications.

Content may include: statements of claim relevant to appeals and applications, name and address.

Sensitive content may include: career related information.

The personal information on these records relates to employees of the Australian Public Service.

The following agency staff have access to this personal information: review committee and support staff.

The records are kept for operational use 1 year.

Some of this information is disclosed to: all parties to an appeal.

Individuals can obtain information regarding access to their personal information by contacting the local offices of the Merit Protection and Review Agency.

The records relate to 11 055 individuals and are stored on paper media.

Location: National and Regional Offices.

2 Record of Public Servants

The purpose of these records is to provide a ready reference to agency officers regarding the full name of participants in promotion appeals.

Content may include: name and information relating to public service employment.

The personal information on these records relates to public servants.

The following agency staff have access to this personal information: all staff.

The records are kept indefinitely.

This information is not usually disclosed to other person or organisations.

Individuals can obtain information regarding access to their personal information by contacting the offices of the Merit Protection and Review Agency.

The records relate to 146 000 individuals and are stored on microfiche media.

Location: Central and State Offices.

3 Grievance and Non-Appellable Promotion Record

The purpose of these records is to investigate grievances under the Merit Protection (Australian Government Employees) Act and the review of non-appellable promotions under the Public Service Act.

Content may include: name and information relating to public service employment.

The personal information on these records relates to public servants.

The following agency staff have access to this personal information: all staff.

The records are kept indefinitely.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting the FOI Contact Officer, Central Office Ph: (062) 571 499.

The records relate to 12 000 individuals and are stored on paper media.

Location: Canberra Office.

4 Division 5 Inquiry Records

The purpose of these records is to enable the Merit Protection and Review Agency to conduct an inquiry in relation to an individuals employment with the Australian Public Service. Such inquiries are conducted under the Merit Protection (Australian Government Employees) Act 1984.

Content may include: name, address and personnel files.

Sensitive content may include: physical or mental health and financial information including debts.

The personal information on these records relates to Commonwealth employees.

The following agency staff have access to this personal information: all staff.

The records are kept for the period of an inquiry.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting the FOI Contact Officer, Central Office Ph: (062) 571 499.

The records relate to an unknown number of individuals and are stored on computer and paper media.

Location: Central Office.

Agency: Public Service Commission

Address: Edmund Barton Building Barton ACT 2600

1 class of records of personal information is held as follows:

1 Personal Files

The purpose of these records is to maintain an employment history for individual staff members for the following work related matters: recruitment, medical assessment, superannuation, salary, leave entitlements, promotion or transfer to other work assignments, work performance reports, disciplinary action, personal injury claims and workers compensation payments.

Content may include: name, gender, date of birth, address, classification, AGS number, rebate, education qualifications, birth/marriage/divorce certificates, recommendation for appointment, probation report, salary deductions, higher duty details and leave details.

Sensitive content may include: physical or mental health, disabilities, racial or ethnic origin, criminal convictions, tax file number, redeployment and retirement details, excess staff arrangements, inefficiency procedures, medical fitness (contested cases), appeal cases (discipline, promotions, redeployment and retirement), grievances on Public Service Commission policy matters, code of conduct matters, withdrawal of resignation and re-appointments, forfeiture of office and other descipline related matters.

The personal information on these records relates to former employees and employees of the Australian Public Service.

The following agency staff have access to this personal information: all staff.

The records are kept permanently.

Some of this information is disclosed to: the Australian Government Retirement Benefit Office, the Department of Industrial Relations, the Department of Prime Minister and Cabinet and Comcare.

Individuals can obtain information regarding access to their personal information by contacting the Privacy Contact Officer Ph: (062) 723 631 or Personnel Manager Ph: (062) 723 604.

The records relate to 20 000 individuals and are stored on computer, paper and microfiche media.

Location: Central Office.

Appendix 5

Proposed Data Registration Form for Hong Kong

Data Protection Ordinance 1995

Application for Registration

B.R. NO……

SECTION A

1. Personal Particulars of Responsible Person for the Data User:

   (a) Name of Responsible Person:

      (i) In English: .....…

      (ii) In Chinese (if applicable): …….

   (b) Correspondence ……. Address:
   ……..

   (c) Designation within the body corporate: ……

   (d) Contact Phone No.: …….

   (e) Contact Fax No.: ……..

2. Personal Particulars of Contact Person:

   (a) Name of Contact Person:

      (i) In English: ……..

      (ii) In Chinese (if applicable): ……

   (b) Correspondence ……... Address: *(if different from that given in 1 (b)*
   ……

   (c) Designation within the body corporate: …….

   (d) Contact Phone No.: ……..

   (e) Contact Fax No.: ……...

SECTION B

This section lists descriptions of the Purposes for which personal data are to be held or used. You will need to complete Section B by putting a tick/ticks in the box(es) in respect of the purpose(s) you wish to register.

Marketing

- ☐ Marketing and Selling (excluding direct marketing to individuals)
- ☐ Marketing and Selling (including direct marketing to individuals)

Management & Administration

- ☐ Working Planning and Management
- ☐ Public Relations and External Affairs
- ☐ Management of Agents and intermediaries
- ☐ Purchase/Supplier Administration
- ☐ Customer/Client Administration

Information

- ☐ Business and Technical Intelligence
- ☐ Research and Statistical Analysis
- ☐ Information and Data Bank Administration
- ☐ Trading in Personal Information

Charity

- ☐ Charity
- ☐ Fund Raising

Property & Estate

- ☐ Property Management and Housing Management
- ☐ Valuation of Real Property

Finance & Banking

- ☐ Share-and Stock-Holding Registration
- ☐ Borrower Account/Credit Facilities Administration
- ☐ Investment/Deposit Account Administration
- ☐ Combined Borrower/Saver Account Administration
- ☐ Personal banking
- ☐ Credit Card and Charge Card Administration
- ☐ Corporate Banking
- ☐ Corporate Finance
- ☐ Lending & Hire Services Administration
- ☐ Investment Management
- ☐ Credit Reference
- ☐ Factoring & Discounting of Trade Debts
- ☐ Accounting and Related Services
- ☐ Statutory Auditing
- ☐ Other Financial Services including Broking

Insurance

- ☐ Life and Health Insurance Administration
- ☐ General Insurance Administration
- ☐ Pensions Administration

Professional Services

- ☐ Legal Services
- ☐ Other Consultancy and Advisory Services

Transport

- ☐ Passenger Transport Operations

Health Care

- ☐ Environmental Health
- ☐ Provision of Health Care
- ☐ Blood Transfusion Services
- ☐ Occupational Health Services
- ☐ Public Health
- ☐ Health Care and Administration

- ☐ Personal/Employee Administration (including Payroll)
- ☐ Membership Administration of Societies
- ☐ Reservations, Bookings and Ticket Issue
- ☐ Education or Training Administration
- ☐ Professional Licensing & Registration
- ☐ Planning and Development Control
- ☐ Grant & Loan Administration
- ☐ Consumer Protection & Trading Standards
- ☐ Social Services/Social work
- ☐ Waste Collection and Disposal
- ☐ Others (please Specify) :.....