THE LAW REFORM COMMISSION OF HONG KONG

PRIVACY SUB-COMMITTEE

REFORM OF

THE LAW RELATING TO INFORMATION PRIVACY

A CONSULTATIVE DOCUMENT

Notice

THIS IS A CONSULTATIVE DOCUMENT, NOT A LAW REFORM COMMISSION REPORT.

It contains the views and recommendations of the Sub-committee on the terms of reference.

The Sub-committee invites submissions upon the document for its assistance and consideration before making its report to the Law Reform Commission.

Now is the time to make your views known.

You are invited to make you submissions in writing before 1 June 1993 to:

The Secretary
The Privacy Sub-committee
The Law Reform Commission of Hong Kong
1/F High Block
Queensway Government Offices
66 Queensway
Hong Kong

The Secretary will be pleased to answer any inquiries concerning submissions.

THE LAW REFORM COMMISSION OF HONG KONG

CONSULTATIVE DOCUMENT OF

THE SUB-COMMITTEE ON PRIVACY

CONTENTS

		Page
INTRODUCTION		1
Terms of Reference		1
What is privacy		1
Membership and method of work		3
Discussion with international experts		4
Layout of the consultative document		5
CHAPTER		
1.	**THE INFORMATION BOOM**	6
	Summary	6
	Computerisation and privacy	6
	New sources of personal data	7
	Anonymity and privacy	7
	Personal records and the control of behaviour	8
	Inaccurate data	8
	The scale of the problem	9
	Public concern about information privacy	9

Automated and non-automated data mediums 10

2. INFORMATION PRIVACY IN THE INTERNATIONAL CONTEXT 12

Summary 12

A. INTERNATIONAL FORMULATION OF DATA PROTECTION PRINCIPLES 13

Introduction 13

International trade in personal data 13

International initiatives to rationalise protection of information privacy 14

OECD 14

The OECD data protection guidelines 15

United Nations Guidelines 17

Council of Europe 17

Commission of the European Communities Draft Directive 18

The data protection principles in Hong Kong 18

B. HUMAN RIGHTS 18

Article 17 of the International Covenant on Civil and Political Rights 18

General comment on art 17 of ICCPR 19

Arbitrary interference 19

Article 17 and information privacy 20

Information concerning a person's private life 20

Relevant decisions of the European Court 21

Article 19 of the International Covenant: privacy vs freedom of information 23

Other competing and interests 24

3. HONG KONG LEGISLATION AND INFORMATION PRIVACY 25

Summary 25

Lack of government records legislation 25

Ordinances With Secrecy Provisions 26

Introduction 26

Inland Revenue Ordinance 26

Census and Statistics Ordinance 26

Secrecy and self incrimination 27

Other ordinances with secrecy provisions 27

Securities and Futures Commission Ordinance 27

Immigration Ordinance 28

Ordinance dealing with family data 28

Rehabilitation of Offenders Ordinance 28

Insurance Companies Ordinance 29

Banking Ordinance 29

Legislation abrogating banking secrecy 29

Credit Unions Ordinance 30

Prevention of Bribery Ordinance 30

Disclosure in the performance of an officer's duties 31

Disclosure of Data Under Ordinances Lacking Secrecy Provisions 31

Introduction 31

Employment Ordinance 32

Education Ordinance 32

Registration of Persons Ordinance 33

Ordinances dealing with health data 33

Legal Aid Ordinance 34

Societies Ordinance 34

Electoral records 34

Ordinances requiring disclosure of financial interests 34

Other ordinances dealing with personal records 34

The UK Official Secrets Act 1989 35

Permissible Limits To Public Authorities Disclosing Information Acquired Under Statutory Powers 35

Bill of Rights Ordinance 39

4. COMMON LAW PRINCIPLES PROTECTION PRIVACY 41

Summary 41

Recommendation 41

Deliberations 41

Historical background 41

The Law of Contract 43

Breach of Confidence 43

Confidentiality and the Purpose Limitation Principle 44

Limitations of the duty of confidence in protecting privacy 44

The media and privacy 45

Relationships and the duty of confidence 46

Contract and the duty of confidence 47

Bankers and doctors: examples of contractual/confidential relationships 48

AIDS and Privacy 51

Disclosure of confidential information in litigation 53

Public interest immunity 53

Professional privilege 54

Confidentiality and copyright compared 54

Defamation 55

Negligence 55

5. INFORMATION PRIVACY IN HONG KONG - THE NEED FOR REFORM 59

Summary 57

Recommendation 57

Deliberations 57

International impetus for data protection 57

A. INTERNATIONAL TRADE IN PERSONAL INFORMATION 58

B. HUMAN RIGHTS TREATY OBLIGATIONS TO PROTECTPRIVACY 58

Present domestic legal status of international privacy norms 59

Present level of legal recognition of data protection principles 59

Collection 59

Disclosure 61

Public sector 61

Private sector 62

Storage 63

Data subject access and correction rights 64

No prospect of major common law developments 65

Voluntary data protection guidelines as an interim measure 65

Feasibility of continued reliance on voluntary guidelines 66

New South Wales: A case study 66

Conclusion 68

6. THE STANDARDS TO BE APPLIED 69

Summary 69

Recommendations 69

Deliberations 70

ECC Draft Directive 72

7. DATA PROTECTION LAWS IN OTHER JURISDICTIONS 78

Summary 78

8. THE OBJECTIVES AND SCOPE OF A DATA PROTECTION LAW 79

Summary 79

Recommendations 79

Deliberations 80

All personal data to be legally regulated 80

Objectives of an information privacy law 81

Principles broader than duty of confidence 81

Regulation of sensitive information insufficient 83

Factual and judgmental data 84

Incorrect data 84

Relevance of data storage mediums 84

The need to regulate non-automated data 85

Unstructured manual records 87

Exemptions 89

9. ENFORCEMENT OF STANDARDS : COLLECTION 90

Summary 90

Recommendations 90

Deliberations 91

OECD Collection Limitation Principle 91

Limiting The Extent Of Collection 92

Only necessary data to be collected 92

Existing data holdings 93

The role of declarations 93

Fair And Legitimate Means Of Collection 93

Purpose Specification Principle 94

Consensual collection: Information data subjects of relevant matters 94

No UK public sector fair obtaining requirement 95

Non-consensual collection: new technologies 96

New technologies, surveillance, and our reference 97

Acquisition from sources other than the data subject 97

Data matching: a paradigm of using pre-collected data 98

A legal requirement of collection from data subject 98

Restricted collection of special categories of data 99

OECD 100

Draft Directive 100

Establishing the sensitive categories of data 100

Mechanisms to restrict the collection of the special categories of data 103

Data processing likely to severely affect the data subject's interests 103

10. REGULATION OF THE USE AND DISCLOSURE OF PERSONAL DATA 105

Summary 105

Recommendations 105

Deliberations 106

Specification of data purposes 106

Alternative approaches to specification of data purposes 107

A NOTIFICATION TO A CENTRAL AGENCY 107

B. NOTIFICATION TO PARTIES OTHER THAN ACENTRAL AGENCY 108

Advantages vs disadvantages of notifying central agency 109

Central notification system preferred 110

Utilisation of business registration scheme 110

Declarations and fair obtaining 112

Non-specification of "obvious uses" 113

Disclosures to be consistent with specified purpose 113

Purpose Specification Principle 113

Data subject consent to incompatible purposes 114

Notification of data subject regarding disclosures 114

Disclosure distinguished from uses generally 115

Deeming data purpose unlawful 116

The ECC Draft Directive's more restrictive approach 117

Data subject control over data relating to him 117

Restricting data purposes adversely affecting data subjects 118

11. PINS AND DATA MATCHING 119

Summary 119

Recommendations 119

Deliberations 120

A. PINS 120

The nature of PINS 120

Functions of PINS 121

Opposition to PINS 121

PINS in Hong Kong 121

Dangers of PINS 122

Overseas responses to PINS 122

The data protection principles and PINS 123

Adequacy of the principles in regulating PINS 124

Legal regulation extending beyond application of the data protection principles 124

Code of practice regulating use of PINS 124

B. DATA MATCHING 125

Profiling and data matching 125

Profiling and the draft Directive 125

Profiling and direct marketing 125

The nature and aims of data matching 127

Data matching and the data protection principles 128

Benefits of data matching 128

Matching and data quality 128

An accurate identifier 129

Accurate data to be matched 129

Valid inferences 129

Concerns about data matching 130

The international control of data matching 130

The draft Directive 131

The need for balance 131

12. DATA QUALITY AND SECURITY 133

Summary 133

Recommendations 133

Deliberations 134

OECD Data Quality Principle 134

Scale of the problem 135

UK Data Protection Act 135

Duty to maintain accurate records 135

Remedying inaccurate records 136

Duty to notify third parties of corrections 136

Data quality and good information practices 137

OECD Security Safeguards Principles 137

The relativity of data security 137

Data security and personal computers 138

Intentional computer misuse 138

Computer Crimes Bill 1992 138

Computer operating error 139

Legal provision for data security 140

13. OPENNESS AND DATA PROTECTION 142

Summary 142

Recommendations 142

Deliberations 143

OECD Openness Principle 143

A. A GENERAL POLICY OF OPENNESS 143

Openness about new developments 144

Legal content of the Openness Principle 144

B. MEANS TO ESTABLISH EXISTENCE OF PERSONAL DATA 146

The role of declarations 146

Contents of declarations 146

Separate entries for each file/database 148

Public access to declarations 149

Indexes of declarations 149

Notification of data subjects 150

Appointment of Responsible Officer 150

14. DATA SUBJECT RIGHTS OF ACCESS AND CORRECTION 151

Summary 151

Recommendations 151

Deliberations 152

OECD Individual Participation Principle 152

Other jurisdictions 153

Our earlier recommendations 154

The mechanics of subject access 154

Material to be provided upon requests 154

Provision of description of data purposes 155

The role of declarations 155

Fees 156

Should the data protection authority set fees 157

Form of request 157

Intelligibility 157

Time limits 157

Limitations on data access 157

Exemptions to data access 158

Giving reasons for claiming access exemptions 159

15. EXEMPTIONS 161

Summary 161

Recommendations 162

Deliberations 163

A. DATA PURPOSES WITH LIMITED PRIVACY IMPLICATIONS 163

Data used solely for private and personal purposes 163

Earlier recommendations 164

Justifications for exempting data solely for personal use 164

Recommendation 165

Non-profit making bodies 165

Other data purposes arguably not infringing privacy 166

Public records 166

B. PUBLIC INTEREST EXEMPTIONS 166

Identifying social interests requiring exemptions 166

Exemptions and the Bill of Rights 167

National Security 168

Recommendations on data held for national security purposes 169

The media 170

Public health and safety 171

Crime and taxation 171

COE recommendations on police data 171

Recommendations on exemptions for law enforcement and tax 172

C. EXEMPTION OF CONFIDENTIAL DATA 172

Confidentiality and access 172

Confidential data with additional public interest aspects 173

Supervision of financial markets 173

Judicial appointments 173

A general access exemption for testimonials 173

Legal professional privilege 174

Confidential health and social work data 174

Indirect access through data protection authority 175

16. STRUCTURE AND POWERS OF ENFORCEMENT AGENCY 177

Summary 177

Recommendations 177

Deliberations 178

The need for an independent enforcement agency 178

International instruments on need for independent agency 179

Human rights Commission a separate issue 180

Recommendation on independent authority 180

Sole responsibility for overseeing data protection 181

Structure of the authority 181

Board of commissioners 181

Independence 182

Adequate budget 183

The cost of data protection regulation 183

Business registration levy 183

17. FUNCTIONS AND POWERS OF THE DATA PROTECTION AGENCY 184

Summary 184

Recommendations 184

Deliberations 188

A. FUNCTIONS OF A DATA PROTECTION AUTHORITY 188

1. INVESTIGATION OF COMPLAINTS 188

Scope of duty to consider complaints 189

False complaints 189

Direct access 189

Form of complaints 190

Class complaints 190

Procedure for hearing data subject complaints 190

Private hearings 191

Legal representation 191

Disposal of complaints 191

Investigations without complaints 192

Commissioner of Administrative Complaints distinguished 192

Remedies for substantiated complaints 193

Compensation for complaints 193

Appropriate body to determine compensation 195

2. ON-SITE INSPECTIONS 195

Inspection and secrecy 197

3. ADMINISTRATION OF DECLARATION SYSTEM 197

Declarations and the data protection principles 197

Declarations and the functions of the agency 197

Avoidance of bureaucracy 198

4. CODES OF CONDUCT 198

5. EDUCATION AND PUBLICITY 199

B. POWERS OF THE PRIVACY COMMISSIONER 200

Introduction 200

Entry to premises 200

Urgent cases 200

Evidence 201

Exempt data 201

Appropriateness of oath requirement 202

C. REVIEW AND APPEAL PROCEDURES 202

18. TRANSBORDER DATA FLOW 203

Summary 203

Recommendations 203

Deliberations 204

A BACKGROUND 204

The need for transborder controls 205

B. TERRITORIAL SCOPE OF DATA PROTECTION LAWS 206

C. REGULATION OF DATA EXPORTS NOT SUBJECT TO GENERAL PROVISIONS OF THE DATA PROTECTION LAW 207

Definition of transfer 208

The draft Directive and permissible data exports 208

Transborder data regulation in other countries 209

Approval requirements 210

Power of intervention to prevent data exports 210

A legal duty on data exporters 211

Methods of satisfying duty to ensure compliance following export 211

Voluntary codes of conduct 211

Contractual assurances of compliance 212

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 document only deals with (a) and (b). The remaining aspects of intrusion and interception will be dealt with in a supplementary document.

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] Law reform inquiries have been of the same view and have opted for an operational approach. So in its 1972 report, the UK committee on Privacy ("The Younger Committee") concluded that as 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 it 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 document.

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 document "personal information" refers to any information relating to an identifiable individual,

---

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

2 Australia Law Reform Commission, *Privacy* (Report No 22), Canberra: 1983, p.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 document 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 document's concern is largely with information records, and also to accord with international usage, "data" will be used unless "information" is more apt.

(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. Its membership is as follows:

---

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

4 Wacks (1989), p.25, see note 1 above.

The Honourable Mr Justice Mortimer, Chairman

Dr John Bacon-Shone, Director, Social Science Research Centre, University of Hong Kong

Mr Don Brech, Director, Government Records Service

Mrs Patricia Chu, Regional Officer (Hong Kong) Social Welfare Department

Mr Con Conway, Director, Major Accounts Group, Hong Kong Telecom

Mr Edwin C K Lau, Assistant General Manager, Retail Banking, Hong Kong and Shanghai Banking Corporation

Mr James O'Neil, Senior Assistant Crown Solicitor, Attorney General's Chambers

Mr Jack So, Executive Director, Hong Kong Trade Development Council (resigned August 1992)

Mr Peter So, Director of Management and Inspection Services, Royal Hong Kong Police Force

Professor Raymond Wacks, Head of Department of Law, University of Hong Kong

Mr Wong Kwok Wah, Honourary Treasurer of the Executive Committee of Hong Kong Journalists Association

Mr Mark Berthold, Senior Crown Counsel, Law Reform Commission (Secretary)

10. The committee's composition reflects the recognition that privacy is a topic raising diverse social issues, requiring the input of diverse opinions. Members have taken the view that it is sometimes necessary to modify or even abandon individual opinions for the sake of a presentation that can be put forward as the best collective view of the sub-committee as a whole.

Discussions with international experts

11. Over a period of two and a half years the committee has reviewed the relevant legal and specialist literature in fifty meetings. This material highlights the international dimension of the protection of privacy. We accordingly considered it essential to discuss the issues with overseas experts, be they involved in the administration of privacy legislation or as commentators. To do this, members attended conferences in Amsterdam and Cambridge in 1991 and the 1992 International Data Protection

Commissioners Conference in Sydney. 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 deep gratitude to all those who met the Sub-committee or supplied it with written material.

Layout of the consultative document

12. The body of this document 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 a limited extent and that as matters stand Hong Kong's legal system provides little protection to privacy. The remainder of the document comprises our recommendations seeking to remedy this situation. Each chapter commences with summary. In the later chapters which contain recommendations, we set out the recommendations immediately after the summary.

CHAPTER 1

THE INFORMATION BOOM

SUMMARY

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.

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

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

(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;

(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.

1.2 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 bases 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.

1.3 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

1.4 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

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

Personal records and the control of behaviour

1.6 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]

1.7 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

1.8 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 information 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 Flaherty, David, *Protecting Privacy in Surveillance Societies* (University of North Carolina Press, 1989), p.9.

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

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

1.9 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

1.10 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 Burnham (1989), p.52, see note 6 above.

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]

1.11 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]

1.12 To what extent these concerns are currently shared by Hong Kong people may be gauged to some extent by the only survey to date 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 also computerisation was comparatively undeveloped. For these reasons, an independent survey will be conducted in March 1993 to coincide with the public release of this document.

Automated and non-automated data mediums

1.13 A major initial decision which the sub-committee has 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.

---

8 Simitis (1987), p.724, see note 5 above.

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

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

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 document 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

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) relevant law on human rights.

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") principles, although the Council of Europe has also promulgated an influential and largely similar model. 25 countries 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 European Communities Commission draft Directive scheduled for implementation in 1994.

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

The International Covenant is narrower in scope than the OECD Guidelines. In particular, it affords protection only to information upon a person's private life. The provision in the International Covenant 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.

A. INTERNATIONAL FORMULATION OF DATA PROTECTION PRINCIPLES

Introduction

2.1 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 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

2.2 The computer boom has already been noted. This 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 export of data to countries lacking adequate data protection. This trend will inevitably accelerate in view of the requirements of the revised draft Directive. Presently scheduled for implementation in mid-1994, the draft Directive requires Member States to provide for restrictions on the export of personal data to third countries lacking an adequate level of data protection. The issue is considered in detail in Chapter 18.

2.3 A related situation is where the exporting country is satisfied that the transfer is likely to lead to a contravention of the data protection principles. The UK 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.[1] The personal data

[1] Dresner, Stewart, "First UK Ban" *Privacy Laws & Business* Winter 1990/1991, p.5.

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).

2.4 It will be seen in Chapter 18 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.[2] 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

OECD

2.5 The Organisation for Economic Co-operation and Development ("OECD") 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:

> *"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;*

---

[2] Nugter, Adriana, *Transborder Flow within the EEC*, (Computer Law Series: Kluwer, 1990) p.204.

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."[3]

The OECD data protection guidelines

2.6 The OECD data protection guidelines ("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 "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.

---

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

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 fulfillment 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.

United Nations Guidelines

2.7 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.

Council of Europe

2.8 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".

Commission of the European Communities Draft Directive

2.9 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.

2.10 The initial draft Directive represented a "first bid". The European Parliament voted on a large number of amendments in March 1992. On October 15 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.

The data protection principles in Hong Kong

2.11 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.

B. HUMAN RIGHTS

Article 17 of the International Covenant on Civil and Political Rights

2.12 The International Covenant on Civil and Political Rights ("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 State 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)). The Hong Kong Bill of Rights Ordinance (Cap 383) ("the BOR") on 8

June 1991 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. 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.

2.13 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. "*

2.14 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."[4] 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.

General comment of on article 17 of ICCPR

2.15 Art 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* [1992] HKCLR 127 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 of the greatest assistance and give them considerable weight." (at p.20)

"Arbitrary interference"

2.16 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*

---

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

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

2.17 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 document. 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 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"

2.18 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. As discussed in Chapter 7, 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[5] 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.

2.19 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.

Relevant decisions of the European Court

2.20 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."*

2.21 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

---

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

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.

2.22 In *Leander v. Sweden* ((1987) 9 EHRR 433) 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.

2.23 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 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.

2.24 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.

2.25 *Gaskin v. United Kingdom* ((1989) 12 EHRR 36) 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 aged one, 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.

2.26 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, 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

2.27 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."*

2.28 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.

Other competing and interests

2.29 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.

CHAPTER 3

HONG KONG LEGISLATION AND INFORMATION PRIVACY

SUMMARY

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.

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.

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

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

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.

Lack of government records legislation

3.1 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.

3.2 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

Introduction

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

Inland Revenue Ordinance

3.4 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.

3.5 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* (1952) 86 CLR 1).

Census and Statistics Ordinance

3.6 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.[1]

Secrecy and self incrimination

3.7 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.

Other ordinances with secrecy provisions

3.8 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.

Securities and Futures Commission Ordinance

3.9 An ordinance whose secrecy provision was relaxed in 1991 is the Securities and Futures Commission Ordinance (Cap 24). In a statement reported in the 19 April 1991 South China Morning Post 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 UK regulators if local brokers were to obtain full authorisation 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.

---

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

Immigration Ordinance

3.10 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 their 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".[2] Upon completion, optical scanners will be installed to read identity cards and travel documents at checkpoints.

Ordinances dealing with family data

3.11 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.

Rehabilitation of Offenders Ordinance

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

---

2 *Hong Kong Standard*, 15 November 1991.

Insurance Companies Ordinance

3.13 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 authorisation enabling the insurer to obtain information from any other source to verify the information provided by the proposer.

3.14 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.

Banking Ordinance

3.15 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.

Legislation abrogating banking secrecy

3.16 There is an increasing legislative trend, however, to enact legislation abrogating bank 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 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. 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. Currently the subject of an appeal to the Privy Council regarding the possible inconsistency of one of its provisions with the BOR, 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.

3.17 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.

Credit Unions Ordinance

3.18 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.

Prevention of Bribery Ordinance

3.19 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* [1987] HKLR 210. The decision of the Court of Appeal has general implications for the exchange of personal information and is examined below. For present purposes it is sufficient to note that it was held that when the ICAC passed on evidence to the Jockey Club for the purpose of disciplinary proceedings it did so with "lawful authority or reasonable excuse".

Disclosure in the performance of an officer's duties

3.20 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* (1952) 86 CLR 1. 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."*

3.21 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. But it would not 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 to eg "obtain revenue". A great number of further functions and duties of IRD staff must be implied if the Ordinance if 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

Introduction

3.22 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.

Employment Ordinance

3.23 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 41B), and detailed employment histories including the employee's identity card number, job title, and wages (section 49). The same section empowers the Commissioner to obtain such of these records as he may require. Nor is the information net extended solely to employees, for section 56 requires employment agencies to maintain records and furnish returns. The data collection net is widened by the Employment Agency Regulations. This requires agencies to compile registers for all job applicants and of all employers who apply for employees, with separate registers to be maintained in respect of employment within and without Hong Kong. Section 58 of the Ordinance confers wide powers on the Commissioner regarding the inspection and copying of the records of employment agencies.

Education Ordinance

3.24 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". But the disclosure provision is 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 examining the feasibility of a system whereby schools will be able to access the Head Office

computer and that the computerisation project was expected to be the biggest yet undertaken by a government department.

Registration of Persons Ordinance

3.25 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. PINs 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 conditioning 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

3.26 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 presently 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

3.27 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 UK Legal Aid Act 1974 which imposes a duty of secrecy without any similar qualification.

Societies Ordinance

3.28 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 earlier 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

3.29 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

3.30 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

3.31 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 UK Official Secrets Act 1989

3.32 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.

3.33 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 UK this right is provided, subject to limited exceptions, by the Data Protection Act 1984. This document recommends that Hong Kong also enact a data protection law.

PERMISSIBLE LIMITS TO PUBLIC AUTHORITIES DISCLOSING INFORMATION ACQUIRED UNDER STATUTORY POWERS

3.34 In their *On the Record: Surveillance*, *Computers and privacy* [3] Campbell and Connor allege that in the UK 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* [1987] HKLR 210. The facts were that Hall, a jockey, had been investigated by the Independent Commission against Corruption ("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

[3] London: Michael Joseph (1986).

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 his Honour:

> *"... 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." (at p.216)*

3.35 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."*

3.36 The other leading judgment 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." (at p.219)*

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

3.38 The judgment of Fuad, J A puts into practice the comment of Sir Robert Megarry, V C in *Malone v. Metropolitan Police Commissioner* [1979] 1 Ch 344 that:

> *"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."*

3.39 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[4].

3.40 *Hall* was followed in *HO Shan Hong v. Commissioner of Police* (1987) HKLR 945. 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 *Marcel v. Commissioner of Police* [1991] 1 All ER 845. 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.

3.41 The ruling arose from a motion for injunctions restraining the police from disclosing to third parties documents obtained without 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*

---

4 Wade, H.W.R. *Administrative Law* 6th edn; (Oxford University Press), pp.399-400.

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." (at p.23)

3.42 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 was 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."*[5]

3.43 *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 they may not extend to Gurry's second category of information, namely that imparted in order to receive a benefit or permission.

3.44 It will be recalled that the OECD data protection guidelines (the Purpose Specification and Use Limitation Principles) requires 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."*

---

5 Law Commission, *Breach of Confidence*, Cmnd 8388, 1981, paragraph 5.31.

3.45 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* [1981] HKLR 352. The court is not bound by decisions of the English Court of Appeal: *de Lasala v. de Lasala* [1979] HKLR 214 (Privy Council). 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

3.46 Enacted in 1991, the Bill of Rights Ordinance (Cap 383) ("the BOR") incorporates into Hong Kong's domestic law the provisions of the International Covenant of Civil and Political Rights ("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 bind 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 disclosure of personal information acquired in the exercise of its statutory powers.

3.47 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."*

3.48 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 2.17 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."*

3.49 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 it. We

saw at paragraph 2.18 above that the quoted expression has a narrower ambit than any information relating to an identifiable individual. But as regards information concerning one'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.*

CHAPTER 4

COMMON LAW PRINCIPLES PROTECTING PRIVACY

SUMMARY

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

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. (paragraphs 4.17 & 4.27)

DELIBERATIONS

Historical background

4.1 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]

4.2 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* (1849) 41 ER 1171. 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."[2] 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. Amongst Commonwealth jurisdictions, New Zealand has been amongst the first to evince support for a tort of privacy. In *Tucker v. News Media Ownership Ltd* [1986] NZLR 716 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".

4.3 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 presently lacking. The English Court of Appeal was confronted in stark terms with the issue in *Kaye v. Robertson* (Unreported: The Times 21 March 1990). 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 him 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.

---

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

2 Wacks, R, *Personal Information: Privacy and the Law* (Oxford, Clarendon Press, 1989), p.82-6.

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

4.4 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 document 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

4.5 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. But even in the absence of express agreement, 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.

4.6 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

4.7 Gurry [3] summarises the requirements of this cause of action as follows:

---

[3] Gurry, Francis, *Breach of Confidence*, (Oxford, Clarendon Press, 1984), p.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 Purpose Limitation Principle

4.8 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

4.9 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 Purpose 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."*[4]

4.10 By comparison, the Purpose 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.

4.11 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

4.12 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."[5] 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 will examine in a later report. It may, however, be useful to point out that, though

---

4 Wacks (1989), p.127, see note 2 above.

5 Wilson, William, "Privacy, Confidence, and Press Freedom: A Study in Judicial Activism" (1990) *53 Modem Law Review*, p.43.

in a number of cases[6] 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 4.13) 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.[7]

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

4.13 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[8] 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* [1988] 2 All ER 545 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 the information. Although the relationship between the parties is frequently important in cases where it is said there is an implied as opposed to express obligation of confidence, the*

---

6 See, for example, *Argyll v Argyll* [1967] Ch.302; *Woodward v Hutchins* [1917] 1 WLR 760; *Lennon v News Group Newspapers Ltd* [1978] FSR 573 and *Khashoggi v Smith* (1989) NLJ 168.

7 See Wacks (1989), p.134, see note 2 above. The inadequacy of the law is examined by Sir David Calcutt (Home Office, *Report on the Committee on Privacy and Related Matters*, Cm 1102, 1990. A follow-up report has just been published.

8 Wilson (1990), see note 5 above.

relationship between the parties is not the determining factor. It 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." (at p.482)

4.14 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[9] "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.'" But in the recent Hong Kong Supreme Court decision of *Koo & Chu* v. *Hing* (unreported: April 14 1992) Bokhary J held that there had been a breach of confidence where not only were the parties not in a relationship, but also where the plaintiffs had not imparted the information to the defendant, it being found by the court that he had obtained it surreptitiously (an appeal has been lodged). The information held to be confidential in that case was not personal information, but questionnaires.

Contract and the duty of confidence

4.15 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." (per Lord Keith in A-G v. Guardian Newspapers (No 2) [1988] 3 WLR 776 at p.781)

4.16 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

---

9 Wacks (1989), see note 2 above.

content from the contractual term, as a result of the former's requirement that the 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

4.17 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.

(i) Banker and Customer

4.18 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* [1924] 2 KB 461. 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."*

4.19 It appears that the contractual obligation of a bank limiting disclosure extends to publicly available information it holds on a customer[10]. 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

[10] Burton, G & Jamieson, P, "Modern Banking Services: Rights and Liabilities" (1989) *63 Australian Law Journal*, p.595.

customers disclose confidential information prior to entering a contractual relationship.[11]

4.20 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[12], 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.[13] 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.

4.21 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

---

11 Walter, J & Erlich, N, "Confidence: Bankers and Customers" (1989) 63 Australian Law Journal, p.404.

12 Australia Law Reform Commission, *Privacy* (Report No 22), Canberra: 1983, p.193.

13 *Banking Services* Cm 622.

of doubtful legal validity have become standard".[14] 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 blacklist of shops suspected of involvement (Apparently those blacklisted were not to be advised). The Jack Committee's recommendations summarised above would, if adopted, 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.

4.22 It is worth noting that the Jack Committee thought its proposals necessary to supplement the protection already afforded by the UK Data Protection Act.

(ii) Medical practitioner and patient

4.23 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 modern 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.[15]

4.24 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* (1986) 85 FLR 118. 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

14 Australia Law Reform Commission (1983), see note 12 above, p.402.
15 Australia Law Reform Commission (1983), see note 12 above, p.415.

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 report 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 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 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 or a professional code addressing the issue of medical research.

AIDS and Privacy

4.25 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 duty of care in negligence to inform partners

potentially at risk (this has been legislated on in California in favour of the latter[16].

4.26 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.[17]

(b) Evidence that leading Hong Kong companies are ignoring World Health Organisation guidelines by testing potential employees for the HIV virus.[18]

(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.[19] 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 UK Medical Defence Union has advised its members to defer to the latter.[20] 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.[21]

4.27 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.**

---

16 See, Pearl, D & S, "Aids: An Overview of the Legal Implications" (1989) 19 Law *Society's Gazette*, p.28.

17 *Hong Kong Standard,* 30 December 1989.

18 *South China Morning Post*, 30 December 1992.

19 *Hong Kong Standard*, 23 March 1991.

20 Pearl (1989), see note 16 above.

21 *South China Morning Post*, 27 & 28 August 1991.

Disclosure of confidential information in litigation

Public interest immunity

4.28 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 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.

4.29 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. So 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* [1982] 2 All ER 791 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 2) [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." (at p.796)

Professional privilege

4.30 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* [1981] AC 1096 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.

Confidentiality and copyright compared

4.31 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* [1983] 2 All ER 101 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 the Television Station 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 s.46(4) of the 1956 Act [applying to HK] expressly provides that 'nothing in

this Act shall affect the operation of any rule of equity relating to breaches of ... confidence'." (at p.117)

Defamation

4.32 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".

4.33 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". But they are assimilated to an extent in those legal systems which provide that a defence of justification or truth should not succeed unless the defendant proved not only 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 privacy is examined in a supplementary document. In the present context, however, it suffices to note that at present Hong Kong defamation law affords very limited protection to information privacy.

Negligence

4.34 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.

4.35 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".

4.36 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.

4.37 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

INFORMATION PRIVACY IN HONG KONG - THE NEED FOR REFORM

SUMMARY

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 International Covenant on Civil and Political Rights be incorporated into Hong Kong's domestic law. The chapter highlights the pressing international trade considerations which argue for early recognition of these standards.

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.

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.

We examine the feasibility of continuing to rely on the existing voluntary controls and conclude, in the light of experience elsewhere, that privacy rights may be eroded without adequate legal controls.

RECOMMENDATION

The internationally agreed data protection guidelines should be given statutory force in both the public and private sectors. (paragraph 5.38)

DELIBERATIONS

International impetus for data protection

5.1 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:

A. International trade in personal information

5.2 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 it 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 its data protection authority to prohibit export when it is not satisfied with the importing country's level of protection. Specific instances were given at paragraph 2.19-20. In one case, the French authority required a contract to be entered into. In the other, the UK authority banned the export of data to the US. 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 will be adopted by 1994. At a more subtle and pervasive level, responsible overseas companies will be inhibited from exporting personal data to Hong Kong.

B. Human Rights treaty obligations to protect privacy

5.3 Article 17 of the International Covenant on Civil and Political Rights ("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"*

5.4 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 reference tasking this Committee to formulate proposals on the matter.

5.5 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 requirement have yet to be given statutory recognition in Hong Kong.

Present domestic legal status of international privacy norms

5.6 The previous chapters have examined the existing legal framework and it is now necessary to scrutinise the extent to which it 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

5.7 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 data protection principles formulated by the Organisation for Economic Co-operation and Development (OECD) 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

5.8 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."*

5.9 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 that it would contravene that also. The ambit of "fair" is less clear. Those

---

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.

means which constitute flagrantly intrusive conduct (eg 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 presently 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.

5.10 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 providing the information may be voluntary in the sense that although provided in response to a request there is no legal compulsion, nor 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.

5.11 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.

5.12 The OECD Data Quality principle, it will be recalled, requires that to the extent necessary for the purposes for which they are to be used, "should be accurate, complete and kept up-to-date." In Chapter 1 (paragraph 1.8) 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 modern technology in rapidly and widely disseminating information, this may be impossible to establish.

5.13 The reliability of information generally deteriorates with age. The answer is regular purging, but computerised systems lack the incentives of pressure of space and storage costs for 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.

5.14 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

5.15 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.

5.16 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 should be subject to the same data protection controls.

Public sector

5.17 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. But 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.

5.18 The duty of confidence may attach to information furnished on a voluntary basis to a public authority. But we have seen that in its decision of

Hall v. ICAC (1987) HKLR 210, the Hong Kong Court of Appeal did not envisage that duty arising when the information is obtained under compulsory powers. The decision could be interpreted as sanctioning public authorities exchanging 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* [1991] 1 All ER 845 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 (that being the particular focus of the Human Rights Committee's general comment).

Private sector

5.19 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 sufficiently certain in scope.

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

5.21 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."*

5.22 This provision was considered by the Court of Appeal in *Tam Hing-yee v. Wu Tai-wai* [1992] 1 HKLR 185. 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. It accordingly further held that it stood repealed by reason of article 3 providing that:

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

5.23 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

5.24 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:

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

5.25 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 presently 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

5.26 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."*

5.27 The OECD Expert Group considers these rights as "perhaps the most important privacy protection safeguard."[2] 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 practical level, such rights of access and correction are vital management tools in enhancing the accuracy of records relied upon in decision making.

5.28 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 US, 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

---

[2] OECD (1981), see note 1 above, paragraph 58.

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. But 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

5.29 The above analysis deals with the extent to which there presently exist in Hong Kong legal provisions, either statutory or common law, giving effect to the internationally agreed data protection principles. We address below the need for legislative intervention. Before doing so, the potential contribution of the courts requires consideration. The question was addressed in *Kaye v. Robertson* (The Times, 21 March 1990 and discussed above at paragraph 4.3). 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. We later consider the possible statutory extension of the common law duty of confidence.

Voluntary data protection guidelines as an interim measure

5.30 The above discussion demonstrates 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 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.

5.31 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

5.32 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 UK 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."[3] That committee reported in 1978 and the international trading impetus for the adoption of domestic legal protection has increased since then.

5.33 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."*[4]

New South Wales: A case study

5.34 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. It is obviously a much stronger voluntary model than that which Hong Kong possesses. But because, unlike Hong Kong, it includes a privacy

---

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

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

agency it is able to monitor the effectiveness of a system lacking legally enforceable controls. It is therefore significant in our view that in a recent annual report[5] it 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 ..."*

5.35 A major inquiry subsequently (and quite independently) completed in that State has highlighted the extent to which privacy protection is eroded in the absence of enforceable controls. In its 2 year inquiry, the New South Wales Independent Commission Against Corruption exposed a widespread corrupt trade in the unauthorised release of government information.[6] 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."[7] 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 precautions have not been taken with the systems that have been in place."[8]

5.36 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*

---

5 New South Wales Privacy Committee Annual Report 1989.

6 New South Wales, Independent Commission Against Corruption; *Report on Unauthorised Release of Government Information*, August 1992. Endnotes 7 to 10 below refer to this Report.

7 Volume 1, Chapter 1, page 3.

8 Volume 1, Chapter 1, page 9.

laws, cherished privacy principles will be at risk, and the scope for widespread corruption will remain."[9]

5.37 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."[10]

Conclusion

5.38 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.**

9 Volume 1, Preface X.
10 Volume 1, Chapter 1, page 8.

CHAPTER 6

THE STANDARDS TO BE APPLIED

SUMMARY

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

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

(ii) the organisation for Economic Co-operation and Development ("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 European Communities Commission's Draft Directive ("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

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 6.1).

DELIBERATIONS

Comparison of texts of OECD Guidelines and Hong Kong Guidelines

	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 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 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.
Use Limitation Principle	Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 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 he 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

	OECD Guidelines	Hong Kong Voluntary Guidelines
		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.
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	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.

	OECD Guidelines	Hong Kong Voluntary Guidelines
	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.	
Accountability Principle	A data controller should be accountable for complying with measures which give effect to the principles stated above.	-----

6.1 **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.

6.2 The precise wording in legislation implementing these principles will be a matter for the Law Draftsman. We note that the UK 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.

ECC draft Directive

6.3 The draft Directive[2] represents the most recent formulation of principles regulating personal data. The first draft was issued on 18 July 1990. The European Parliament proposed a number of amendments and on 15 October 1992 the Commission issued an amended version to take into

---

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

2 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.

account Parliament's opinion. References in this document to the text of the draft Directive are to the revised version. The structure of the draft Directive differs somewhat from the OECD formulation. While article 6 contains a statement of data protection principles, they are more tersely expressed than the OECD guidelines. They are supplemented, however, by article 7's articulation of the grounds on which personal data may be lawfully processed. The full text of the two provisions are as follows:

> *"Chapter II*
>
> *General Rules of the Lawfulness of the Processing of Personal Data*
>
> *ARTICLE 5*
>
> *Member States shall provide that the processing of personal data is lawful only if carried out in accordance with this Chapter.*
>
> *Subject to this Chapter, Members States may more precisely determine the circumstances in which the processing of personal data is lawful.*
>
> *Section I*
>
> *Principles Relating to Data Quality*
>
> *ARTICLE 6*
>
> *1. Member States shall provide that personal data must be:*
>
> *(a) processed fairly and lawfully;*
>
> *(b) collected for specified, explicit and legitimate purposes and used in a way compatible with those purposes;*
>
> *(c) adequate, relevant and not excessive in relation to the purposes for which they are processed;*
>
> *(d) accurate and, where necessary kept up to date; every step must be taken to ensure that data which are inaccurate or incomplete having regard to the purposes for which they were collected are erased or rectified;*
>
> *(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes in view; Member States may lay down appropriate safeguards for personal data stored for historical, statistical or scientific use.*

2. It shall be for the controller to ensure that paragraph 1 is complied with.

Section II

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;

(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."

6.4 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."[3] 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.

[3] Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris: OECD, 1981, paragraph 55.

CHAPTER 7

DATA PROTECTION LAWS IN OTHER JURISDICTIONS

SUMMARY

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.

7.1 The following 25 countries 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:

Country	year came into force
Australia	1988
Austria	1978
Canada	1982
Czechoslovakia	1992
Denmark	1978
Finland	1987
France	1978
Federal Republic Of Germany	1977
Guernsey	1986
Hungary	1989
Iceland	1981
Ireland	1988
Isle of Man	1986
Israel	1981

[1] Dresner, Stewart, Privacy *Laws & Business.*

Country	year came into force
Japan	1988
Jersey	1987
Luxembourg	1979
Netherlands	1988
New Zealand	1991
Norway	1980
Portugal	1991
Sweden	1973
Switzerland	1992
United Kingdom	1987
USA	1974

7.2 It will be observed that European countries predominate to date, although North America is also represented. Both regions, of course, are fully industralised. The only Pacific rim countries represented to date are Australia and Japan.

7.3 In addition to these countries which have enacted laws on the matter, a number of others are actively considering legislating. Bills have been prepared in Belgium, Greece, Italy, Poland, and Turkey.[2]

7.4 As already mentioned, a data protection law is one that enforces the data protection principles as regards personal information records. How they set about doing this varies a great deal. Some of the major differences are as follows.

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

7.5 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.

Direct enforcement by data subject litigation vs enforcement agency

7.6 With the sole exception of the USA, the different laws establish a specialised agency 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 document will refer to the regulatory agency envisaged for Hong Kong as the "Privacy Commissioner". This does not of course pre-empt the adoption of a more suitable term at a later date.) To

[2] Dresner, Stewart, Privacy *Laws & Business.*

equip them to discharge their enforcement role, they are conferred powers of varying width regarding such matters as inspection of data users. These agencies 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

7.7 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 legislating to regulate the private sector, although the US and Australian federal governments have enacted legislation to regulate specific private sector records, such as credit records.

Advisory or mandatory enforcement powers

7.8 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 UK 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

7.9 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 such approval requirements are generally referred to. The 1988 Netherlands law, for example, only requires data users to notify its supervisory authority of its activities, consent not being required. Also, the recent Home Office review of the UK 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.

CHAPTER 8

THE OBJECTIVES AND SCOPE OF A DATA PROTECTION LAW

SUMMARY

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.

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, although we later recommend that such data have additional protection.

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 it is 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

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 8.12). The data to be regulated must, however, be systematically disposed in such a way as to enable access to required data to be practicably obtained whether by automated means or otherwise (paragraph 8.28).

DELIBERATIONS

All personal data to be legally regulated

8.1 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" is 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" are wider 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.

8.2 It follows that for the purposes of regulation "personal data" refer 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]

---

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

2 Wacks (1989), see note 1 above, p.25.

8.3 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

8.4 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.

(i) Regulation of data representing information

8.5 The first thing to notice 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* [1988] 2 All ER 545 (discussed above at paragraph 4.13) 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 regulate the disclosure of recorded information, although the disclosure itself may be in any form, including orally.

Principles broader than duty of confidence

8.6 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 Purpose Limitation Principle. We saw in Chapter 4 that insofar as

---

[3] Wacks (1989), see note 1 above, p.16.

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

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 modem 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 he will accordingly be disposed to limit disclosure to the record. Should the record keeper orally add extraneous comments about the data subject which do not constitute disclosure of the record, such comment 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.

(ii) Fair information practices

8.7 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."[5] 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 (eg denial of credit), access and correction rights enable him to provide periodic inputs.

(iii) Informational self-determination

8.8 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 "[6]

---

5 Aronson, M & Franklin, N, *Review of Administrative Law* (Sydney: The Law Book Company Limited, 1987), p.91.

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

Regulation of sensitive information insufficient

8.9 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 this quality. 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 European Communities Commission draft Directive ("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."*

8.10 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 history has recently confirmed may be the basis of discriminatory policies (as Milan Kundera has written [7], "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.

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

8.12 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.** 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.

---

[7] Kundera, *The Book of Laughter and Forgetting*, London: Penguin Books, 1980).

8.13 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

8.14 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

8.15 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 it purports to be strictly factual or contains an evaluative aspect. Indeed, the Openness Principle confers the right of data subjects 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".

8.16 The application of the data protection principles to both inaccurate as well as accurate data demonstrates that they 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

8.17 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 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 its 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

8.18 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

8.19 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 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 the test that the law only apply to data in whatever format which is reasonably readily retrievable.

Operational interrelationship between mediums

8.20 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 the automatic non-automatic handling of data. They noted that there are "mixed" data processing systems.[8] 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. Jon Bing 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.[9]

Manual records still dominant in public sector

8.21 In Hong Kong, non-automated records still dominate in the public sector. The total quantity of records held by government agencies totals some 423 kilometres. Files comprise 54 % of this total and only 1 % is presently machine readable. Although rapid computerisation of new government records is under way, clearly the failure to apply the law to non-automated records would emasculate public sector regulation for the foreseeable future.

Opportunity of evading regulation

8.22 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."*[10]

Circumvention may be effected by moving personal data from databanks onto manual records or simply refraining from computerising manual information.

---

8 OECD (1981), see note 6 above, paragraph 35.
9 *Privacy Laws & Business Newsletter* (October 1990), p.5.
10 OECD (1981), see note 6 above, paragraph 35.

There is evidence that the latter is occurring with UK employment-vetting agencies, for example.[11]

Much information recorded manually

8.23 Often it is the more intimate information 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 our 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. In 1984 it enacted the Data Protection Act. Contrary to the recommendations of the Lindop Committee, it restricted its attention to the automatic processing of data. Subsequent enactments in 1987, 1988, and 1990, however, have granted access and correction rights in relation to social services, housing authorities and health records. This ad hoc approach has been criticised[12] 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.

Unstructured manual records

8.24 Non-automated records range from the systematic to the shambolic. The extent to which they are structured 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 it poses 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 with 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 an on-going basis of decisions affecting him by the record-keeper. The same retrieval difficulties reduce the incidence of its transmission to other decision makers.

8.25 Turning from principle to practicability - and the practicability of our proposals is of vital concern to us - we are concerned that to apply 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

---

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

12 *New Law Journal*, 5 October 1990, p.138.

the record keeper having to sift through large amounts of material for scattered references to the data subject.

8.26 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."*

8.27 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 Mr Brech of our committee advises 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.

8.28 In view of the above **we recommend that the data protection law apply to personal information contained in an organised collection of data in whatever form which is systematically disposed in such a way as to enable access to required data to be practicably obtained by automated means or otherwise.** 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 satisfying the accessibility test will be regulated whether it appears 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 and which are accordingly vulnerable to being outstripped by future developments.

8.29 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.

8.30 This definition of organised records contained in our recommendation is similar to that in article 2(b) of the draft Directive. The only significant difference is that the data must "enable" access rather than

"facilitate" it. Our formulation is therefore slightly narrower, because the former connotes making possible whereas the latter conveys merely making easier.

Exemptions

8.31 We have delineated 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

ENFORCEMENT OF STANDARDS: COLLECTION

SUMMARY

Data processing begins with its acquisition or collection. Collection may be from the data subject, or a third party, or by transfer of pre-collected data from these sources. 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.

The data collection principles require that limits be set on the collection of personal data. We address the need to restrict collection to data 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, which may be absent when data is collected from third parties. We consider, but reject, a qualified requirement of direct collection. The collection of sensitive data should be the subject of supplementary controls. Data may be sensitive because it pertains to initimate 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.

RECOMMENDATIONS

(i) There should be a legal requirement along the lines that:

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

(b) the collection or storage is necessary for or directly related to that purpose (paragraph 9.5).

The legislation should provide a suitable transition period to enable organisations to review their holdings and comply before sanctions become applicable. (paragraph 9.6)

(ii) When data are collected directly and with the knowledge of the data subject, he should 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 (paragraph 9.13)."*

(iii) A data subject from whom data are collected without his knowledge through remote monitoring should be informed of the frequency of data collection, the time of its storage, and the use to be made of the data. If this is not feasible, the collection of data should be subordinated to legal authorisation (paragraph 9.19).

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

> the data subject's consent should be required prior to the installation of the relevant (videotex) technology in his residence.
>
> only personal information which is necessary for service or billing purposes should be collected and stored (paragraph 9.20).

(v) The data subject's consent should be required to 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 (paragraph 9.43).

DELIBERATIONS

OECD Collection Limitation Principle

9.1 It will be recalled that the OECD Collection Limitation Principle 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."

9.2 This principle has several main concerns. The first is with limiting the extent of collection. The second is the legitimacy of means employed to obtain data within those limits. Related to this is the role of consent. These aspects will now be examined.

LIMITING THE EXTENT OF COLLECTION

Only necessary data to be collected

9.3 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 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."[1] 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 if they are relevant and therefore *necessary* for its 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. "

9.4 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.

9.5 In view of the above, we favour statutory recognition being given to the requirement that only relevant information be collected in both the

---

[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.

public and private sectors. **We accordingly recommend a provision on the following lines:**

> **that personal data shall not be collected or held unless:**
>
> **(a) the data are collected or held for a lawful purpose directly related to a function or activity of the collector; and**
>
> **(b) the collection or storage is necessary for or directly related to that purpose.**

Existing data holdings

9.6 The inclusion in the above recommendation of a reference to existing records recognises that in Hong Kong much personal data have already been collected and is presently held. In our view, the same requirement of relevance should apply to these holdings. **We recommend that the legislation provide a transition period to enable organisations to review their holdings and comply before sanctions become applicable.**

9.7 Article 7 of the draft Directive goes on to provide that the processing (including collection) of personal data should only take place if the data subject consents, is necessary for the performance with the data subject or for the protection of his "vital interests", or:

> *"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."*

9.8 This restriction in article 7 of data purposes is dealt with in the next two chapters.

The role of declarations

9.9 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 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

9.10 The OECD principle requires that data should be obtained 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 having been 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

9.11 The Collection Limitation Principle adds that collection should be "where appropriate, with the knowledge or consent of the data subject". But this knowledge or consent cannot operate in a vacuum: it must relate to the purpose that the data are collected for. 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."*

9.12 It follows that if data are to be collected with the knowledge and consent of the data subject, he must be informed of its 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

9.13 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 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".

9.14 This provision embodies what the Council of Europe refers to as the "free and informed consent of the data subject".

No UK public sector fair obtaining requirement

9.15 It is worth noting the provisions of the UK Data Protection Act on the issue, as they presently diverge in a major respect from the draft Directive provision. In common with many data protection statutes and our own model, the core of the UK legislation consists of a set of data protection principles. Their precise wording follows the Council of Europe Convention's formulation rather than that of the OECD, but they cover similar ground. The principle dealing with collection in the UK Act states that "the information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully". As with the other very generally worded principles, it is elaborated on in the interpretation guide of the Act. This provides that regard shall be had to whether the person from whom the information was collected was deceived or misled as to the use that will be made of it. The UK Data Protection Registrar has expressed the view that the draft Directive provision is similar in effect to the UK fair obtaining requirements, although the draft "is stricter and less flexible".[2]

9.16 The UK Act's fair collection provision differs from the draft Directive provision by exempting those acting under statutory authority. It does so by deeming information to be obtained fairly if its collection is authorised or required by statute. Even prior to the release of the draft Directive, the Registrar argued that this complete exemption is "too sweeping and may license practices which on their merits would be unacceptable in other circumstances".[3] He observed that UK authorising legislation does not generally include counterbalancing codes for collection. The Hong Kong legislation reviewed in Chapter 3 is similarly lacking. He accordingly recommended that acting under statutory powers raises a rebuttable presumption that the information has been fairly obtained. The presumption would be rebutted where it was shown that the fair collection principle would not be likely to prejudice the statutory purpose for which the data were being obtained. As with the other proposals to overhaul the UK Act, its fate will be determined by the final shape of the Directive and the UK Government's stance towards it.

---

2 *Fifth Report of the Data Protection Registrar*, June 1989, London: HMSO.

3 Data Protection Registrar (1989), see note 2 above, paragraph 68.

9.17 In our view, article 11 provides a useful articulation of fair consensual collection. It applies equally to both the public and private sectors. We agree with this approach, not only in this context but generally. The categories of information of which the provision requires disclosure will ensure the data subject's informed consent. We recognise the danger that rather than fulfil its requirements, data collectors will prefer to rely on pre-collected data, or data provided by third parties. We also consider that it should apply equally to the public and private sector. We note that this is required by the French provision (section 27) which article 13 resembles. In particular, we are reluctant to place the onus on data subjects of rebutting a presumption of fair obtaining by statutory authorities. We note that article 11 contains a proviso to accommodate public sector functions. **We recommend that article 11 be given statutory effect.**

Non-consensual collection: new technologies

9.18 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.[4] It recommends that individuals to be 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 authorisation. The recommendation goes on to prohibit the secondary use of the data and 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.

9.19 We propose that the collection of data from data subjects by remote 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 remote 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 non-remote 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

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

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.

9.20 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 remote 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 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:**

> **the data subject's consent should be required prior to the installation of the relevant (videotex) technology in his residence.**
>
> **only personal information which is necessary for service or billing purposes should be collected and stored.**

New technologies, surveillance, and our Reference

9.21 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. As this example demonstrates, it is increasingly artificial to distinguish data protection issues from other privacy issues.

Acquisition from sources other than the data subject

9.22 The requirement that data be collected with the data subject's knowledge or consent implies that where appropriate it should be collected from the data subject, rather than from another source. This ensures the data subject's knowledge or consent. 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."[5]

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

9.23 The general question of data matching is considered in Chapter 11. For present purposes, the relevant point is that matching data collected in different contexts may negate the requirement that collection be with the data subject's knowledge and consent. Compared with direct collection, it is also prone to problems regarding the meaning and quality of the data being matching. 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."[6]

9.24 It follows that direct collection will often best ensure compliance with another data protection principle considered below, namely the Data Quality Principle.

A legal requirement of collection from data subject?

9.25 In view of the above, we have considered whether there should be even a qualified legal requirement of direct collection from data subjects. We note that 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

---

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

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

personal data have to be collected directly from the data subject." [7] Collection by third party transfers is widespread, however, and it may be neither realistic nor indeed practical to attempt to ban it. Jon Bing has identified the factors favouring the use of previously collected information.[8] Such pre-collected information is readily accessible. Consensual 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 accordingly decline to make a general recommendation to this effect. 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.

Restricted collection of special categories of data

9.26 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.

9.27 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 its 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 (eg 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*

---

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

8 Bing (1991), see note 6 above.

changes is the extent to which he is prepared to permit the information to become known or used."[9]

OECD

9.28 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 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".[10] One of the relevant considerations in such an exercise was the "traditions and attitudes in each member country."

Draft Directive

9.29 Article 8 of the draft Directive goes further than the OECD principle and expressly restricts the collection of 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."*

9.30 This provision raises the question of whether the collection of certain classes of data should be limited. There are two issues:

(i) identification of the categories of data whose nature is such that its collection should be restricted; and

(ii) the appropriate mechanism for controlling collection.

Establishing the sensitive categories of data

9.31 Article 17 of the draft Directive restricts the collection of two conceptually distinct categories of 'sensitive' information. These are intimate data and data likely to be utilised in discriminatory decisions:

---

9 Wacks, R, *Personal Information: Privacy and the Law* (Oxford, Clarendon Press, 1989), p.23.

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

1. Intimate data

9.32 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."*[11]

9.33 It is commonly pointed out that notions of the sensitivity of data is 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. Whilst it is probable that most people in Hong Kong are discreet about their sexual activities, there will no doubt be those that boast about them. Regulation, however, is neither practicable nor justifiable unless it relates to the commonly held expectations of the community. It is the expectations of "reasonable" rather than eccentric citizens which is relevant when identifying the categories of sensitive data. This approach requires empirical data on what the Hong Kong populace considers sensitive. As regards the two categories of intimate data identified by article 8, namely that concerning health or sexual life, we think that they are considered as sensitive in Hong Kong as elsewhere. We welcome, however, views of the public on what categories of data are considered sufficiently sensitive to require special controls.

9.34 The further question is whether the collection of such 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."*[12]

9.35 Limiting the collection of intimate data is an effective method of redressing this.

---

11 Wacks (1989), see note above, p.229.

12 Wacks (1989), see note above, p.205.

2. Data relating to discrimination

9.36 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."*[13]

9.37 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.

9.38 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.

9.39 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 the appropriate mechanism to restrict the collection of such data.

---

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

9.40 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."

9.41 The issue remains whether the special categories of data should be restricted to those identified by article 8. There appear to be two alternatives:

(i) accompanying the specific categories identified by article 8 with a general formulation of sensitive data along the lines of that proposed by Professor Wacks.

(ii) Identifying the other categories of data which are considered sensitive in Hong Kong. This would require empirical research. It would, however, result in firm legislative guidance being provided on the point.

Mechanisms to restrict the collection of the special categories of data

9.42 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.

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

9.43 We reject (i) as a realistic option. Nor are we persuaded at this stage that the remaining two options should be adopted. Of the two we prefer (iii). This is because involving the data protection authority in a consent role would encourage bureaucracy. **We recommend that the consent of the data subject be required for the collection of sensitive data.** We also seek views of the public on precisely what categories of data are considered sensitive in Hong Kong.

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

9.44 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 give 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."[14] 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."[15] This would encompass the identification of "hits" by means of the investigative data matching techniques discussed at paragraph 9.22 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.

---

14 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.

15 CEC (1992), see note above.

CHAPTER 10

REGULATION OF THE USE AND DISCLOSURE OF PERSONAL DATA

SUMMARY

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, whose approval may be required. 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

(i) 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 10.12)

(ii) 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 10.15) The form should also alert applicants holding personal data of the need to complete a supplementary form available at the Business Registration office. This form should require the specification of the basic features of the personal data held, including a specification of its purpose(s). (paragraph 10. 6)

(iii) Government and public authorities, together with private sector organisations using of personal data, not subject to business registration requirements, should be required to notify the Privacy Commissioner direct, by furnishing him with their declarations. (paragraph 10.18)

(iv) 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 10.18)

(v) Data subjects should not be deemed to have knowledge of specified data uses contained in public declarations. (paragraph 10.19)

(vi) 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 a statutory provision to the contrary, including one of the non-disclosure exemptions discussed in Chapter 15. (paragraph 10.22)

(vii) "Data subjects 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 recipient of the personal 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. (paragraph 10.26)

DELIBERATIONS

Specification of data purposes

10.1 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."*

10.2 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)

10.3 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

10.4 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.

A. Notification to a central agency

10.5 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:

(i) Notification but no approval requirement

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

---

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

2 Home Office (1990), see note 1 above.

(ii) Notification coupled with approval requirement

10.7 This approach encompasses both the so-called "registration systems" and "licensing systems". The difference is that the former does not require approval prior to the processing of data, whereas the latter does. Sweden is one of the few countries with a licensing system. Registration systems are more common, and the present UK 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.

(iii) The draft Directive's mix of (i) and (ii)

10.8 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, however, 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.

B. Notification to parties other than a central agency

10.9 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:

- a statutory declaration made to a solicitor

- verification and dating of a document by a professional person such as a banker or accountant

- publication, for example in the organisation's annual report or a newspaper with a verifiable date of issue

- 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.)

- 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 central agency

10.10 The principal advantages of such a scheme which have been identified by the UK 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]

10.11 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 UK law totally abandon its present approval ("registration") requirement, but that it should not be replaced by the requirement that the

---

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

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

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 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

10.12 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.**

10.13 In determining the appropriate notification arrangements, we have borne in mind the following principles:

(i) effectiveness

(ii) simple and appropriate procedures

(iii) minimal cost and bureaucracy

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

Utilisation of business registration scheme

10.14 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, craftmanship, 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. Upon completion, the form

---

5 *Transnational Data and Communications Report*, May 1991, p.41

6 *Transnational Data and Communications Report*, March 1991, p.47

7 *Transnational Data and Communications Report*, January, 1992.

is returned to the Business Registration office for entry into one of their computing systems.

10.15 **We recommend that the Business registration scheme should be made the principal means of identifying holders of personal data and bringing them within the scope of regulation.** There are over 300,000 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 in the following way:**

> *"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 hanged in the last year?"*

10.16 Hong Kong has a large number of sole proprietors, a number of whom 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 also alert these 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 item requiring description is that of the purpose(s) for which the data are held.** We recommend in Chapter 13 that in addition, a very brief description is required of the types of data held, classes of data subjects, classes of persons to whom the data are usually disclosed, and the countries to which the data are exported. 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.

10.17 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.

10.18 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. (In paragraph 15.7 below we recommend an exemption from this requirement for non-profit making organisations where the data relates solely to its members and is not communicated to third parties.) 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 principle 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.**

Declarations and fair obtaining

10.19 It may assist to clarify the status of specification of purposes contained in a declaration. In the last chapter we recommended that individuals from whom personal data are collected be informed of its proposed uses etc (paragraph 9.14). 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 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.**

10.20 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. But this would simply be a question of fact and not conclusively determined by the contents of the declaration.

Non-specification of "obvious uses"

10.21 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 commonly engaged in activities. 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.

DISCLOSURES TO BE CONSISTENT WITH SPECIFIED PURPOSE

Purpose Specification Principle

10.22 **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."***

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

> "*3. Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes."*

10.24 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.

Data subject consent to incompatible purposes

10.25 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."*

10.26 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 together with its 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."**

Notification of data subject regarding disclosures

10.27 Article 12 of the draft Directive adds a further condition on the processing of data in the private sector. It 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 Netherlands laws 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 be the explanation why people we spoke to in those two countries had only rarely received such notifications.

10.28 We have considered whether to also adopt a general legal requirement that data subjects be notified when data relating to them is stored or communicated for the first time. We recognise that the aim of the requirement is to increase the transparency of data processing. The issue is more fully considered in a later chapter on the rights of data subjects, including access rights. We there recommend that data subjects be provided access rights to data relating to them. We have already recommended above that when data are collected directly from data subjects, they be informed of the uses to which it will be put. We have also recommended above that all record keepers compile declarations which will be publicly available. The combined effect of these measures will be to provide a sufficient degree of transparency without the additional general requirement of notification proposed by article 12.

Disclosure distinguished from uses generally

10.29 The OECD guidelines subject the use 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 UK Act, however, it attaches the special obligation regarding disclosure of notification to the data subject. We disagree above with that method, but have nonetheless considered whether it is appropriate for a data protection law to 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 the amount of data that is disclosed, rendering personal data anonymous whenever possible, and the logging of particularly sensitive disclosures.

10.30 We also note that the Australian Privacy Act 1988 recognises the additional need for care with disclosures. Thus its 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. "Use" is defined in the Australian provision as not including disclosure, this being specifically dealt with in the principle which provides in part 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:*

---

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

(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 …"

10.31 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 its proposed purposes.

10.32 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 for two reasons. First, we recommend below in Chapter 13 that one of the classes of information to be included in declarations shall be the classes of persons to whom the data are usually disclosed. As we have recommended declarations to be public documents to which data subjects will have ready access, this should provide the data subject with sufficient notice of persons to whom data are transmitted. Second, our main concern regarding disclosure is that a mechanism should exist to ensure that transferees are notified of corrections of inaccurate data. We recommend such a mechanism in the next chapter.

Deeming data purpose unlawful

10.33 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]

---

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

10.34 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 ECC Draft Directive's more restrictive approach

10.35 It is against this backdrop that the draft Directive provisions must be considered. It does not set out separately equivalents of the Use Limitation and Purpose Specification Principles. Article 6(b) provides for their combined operation, namely 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

(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

10.36 The conditions stipulated in (a)-(d) 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* sums up this approach as follows:

> *"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

10.37 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 other five limbs of that provision). The draft Directive has other, more specific, provisions to the same effect. In the last chapter we endorsed the provision requiring data subject consent to the processing of the sensitive categories of data. We also noted that 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 further draft Directive provision requiring data subject input before adverse decisions are taken on the basis of profiling. 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 consent of the data subject or the approval of the data protection authority.

---

10 Home Office (1990), see note 1 above.

CHAPTER 11

PINS AND DATA MATCHING

SUMMARY

This chapter discusses two related concerns:

(i) the information privacy implications of personal identity numbers ("PINs"); and

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

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. PINs 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 PINs should correct the present excessive collection and use.

Matching across databases 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.

Profiling may also expose the data subject to adverse consequences and we conclude that it should similarly be accompanied by procedural safeguards, albeit less stringent ones.

RECOMMENDATIONS

(i) The use of PINs 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 PINs. (paragraph 11.7)

(ii) The Privacy Commissioner should promulgate a code of practice on the use of PINs. The code should make explicit the application of the data protection principles to the use of PINs, including the ID card number. The Privacy Commissioner should take into account the terms of the code when investigating complaints. (paragraph 11.11)

(iii) The data subject should have the right not to be subjected to an adverse administrative or private decision (except pursuant to a contract) adversely affecting him which is based solely on an automatically processed

profile relating to him. The data subject should be allowed to put his point of view prior to the adverse decision being taken. (paragraph 11.14)

(iv) The data user's controller should expressly offer the data subject the opportunity to have data erased without cost before the data are disclosed to third parties or used on the behalf of the data subject for the purposes of marketing by mail. 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. (paragraph 11.16)

(v) Investigative data matching involving the comparison of data to identify "hits" should be subject to the following safeguards:

> 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 supervisory authority should promulgate mandatory guidelines setting out the relevant factors in determining whether approval shall be granted. These will include the nature and sensitivity of the personal data, its expected accuracy, and the seriousness of consequences of being identified as a "hit". Also relevant is whether it is proposed to inform data subjects in advance.
>
> The guidelines should also set out procedures according "hits" the right to correct matching results before adverse decisions are taken on their basis.
>
> 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 that are less satisfactory, and a cost/benefit analysis of the programme. (paragraph 11.35)

DELIBERATIONS

A. PINS

The nature of PINS

11.1 As PINs 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 PINs 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 PINS

11.2 The main purpose of PINs 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, it may be a multi-purpose PIN. The Hong Kong ID card number is an example of the latter. The data protection danger arising from a multi-purpose PIN resides in its capacity to facilitate the linking of data across different sectors. In both cases, however, PINs 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 PINS

11.3 A chief danger of PINs 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 PINs 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]

PINS in Hong Kong

11.4 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

---

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

2 COE (1989), see note 1 above.

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

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 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." But through a gradual process of extension, Hong Kong residents are now routinely subjected to private sector requests for the number as a matter of course when completing transactions.

Dangers of PINS

11.5 It would appear that Hong Kong people are habituated to the use of 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, involving 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, they 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 PINS

11.6 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 PINs 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 PINS

11.7 PINs such as the Hong Kong ID card number constitute personal data, as it relates to an identifiable individual. They are therefore susceptible to the application of the data protection principles. **For the avoidance of doubt, we recommend that the use of PINs be regulated in the same manner as any other item of personal data and that our other recommendations should be interpreted as applying to PINs.** 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 it will be used, the obligatory or voluntary nature of the requests for data, the consequences if they fail to reply, and the recipients of the information;

11.8 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 PINS

11.9 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 the principal danger posed by their use, namely data matching. We now set out our reasons for adopting the intermediate approach.

Legal regulation extending beyond application of the data protection principles

11.10 The legal regulation of the use of ID numbers could be in the form of a prohibition on requiring its 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 as outlined in paragraph 11.7 above.

Code of practice regulating use of PINs

11.11 While in principle the general application of the data protection principles should provide the necessary protection against misuse of PINs, 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 PINs. This would both usefully highlight the issue, and clarify possible ambiguities. An example of the latter may be whether the purpose of disclosing an ID number should be taken to extend to facilitate matching. In our view the code should explicitly provide that it should not so extend. 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 agency established to oversee data protection in Hong Kong promulgate a code of practice on the use of PINs. The code would make explicit the application of the data protection principles regarding PINs, including the ID card number. The data protection authority would take into account the terms of the code when investigating complaints.**

B. DATA MATCHING

Profiling and data matching

11.12 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 is compared with what he said on another. Indeed, often "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

11.13 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] "*

11.14 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. **Upon this basis, we recommend adoption of this requirement.** 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.

Profiling and direct marketing

11.15 We accept that profiling may assist in the accurate identification of goods and services, resulting in a reduction of their cost. We also recognise that data subjects identified in this manner may object to becoming targets of direct mail. We note that the UK Data Protection Registrar reports that a significant percentage of complaints received are about unsolicited mail, although the percentage has dropped from 44.5% to 18.5% over the last three years.[4] Although the draft Directive does not consider direct mail as a sufficiently adverse consequence to merit the controls contained in the profiling provision quoted above, it addresses the issue elsewhere. Article 15(3) provides:

---

4 Eighth Report of the Data Protection Registrar, June 1992, London: HMSO.

"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."

11.16 This provision does little more than make explicit the general requirements of the data protection principles, namely those relating to using data consistently with the purpose for which it was originally provided. We agree, however, that it is useful to spell out their application to this increasingly common form of commercial activity. **We recommend its adoption. We further recommend 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.**

The nature and aims of data matching

11.17 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 raise the same issues and our recommendations do not differentiate between them.

11.18 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.

11.19 Other private sector matching is less 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 the sending of customers multiple

copies of the same advertising material. It may even be for the positive purpose of identifying incorrect data and its subsequent correction.

Data matching and the data protection principles

11.20 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 it was 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.

11.21 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.

Benefits of data matching

11.22 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 programmes may have a deterrent effect on dishonest claims. A similar justification obtains in the private sector credit and insurance industries.

Matching and data quality

11.23 The accuracy of a matching programme is dependant on:

(i) an accurate identifier

(ii) accurate data to be matched

(iii) valid inferences drawn from the matching

These factors will now be examined.

An accurate identifier

11.24 The accuracy of a matching programme 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 a 5 % plus error factor, 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.

Accurate data to be matched

11.25 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:

- whether the meaning of key terms such as "income" varies according to context. A graphic example of such variation was provided in para 9.23 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."

- 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.

Valid inferences

11.26 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. This is relevant to the issue considered below of whether "hits" should be accorded procedural safeguards.

Concerns about data matching

11.27 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.

The international control of data matching

11.28 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.

11.29 Data 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:

- prior cost-benefit analyses of matching programmes, including reference to potential impact on privacy;

- advance notification to Privacy Commissioner;

- approval required by the responsible minister;

- public gazetting of all matching programs; and

- verification of adverse findings before taking administrative action.

11.30 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 UK Data Protection Registrar addresses the issue in his latest annual report and concludes that it may now be an appropriate time to regulate matching.

11.31 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 matching programmes.

The draft Directive

11.32 Although it does not use the term "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."*

11.33 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

11.34 In view of the above, we view data matching as a procedure which poses a number of data protection dangers and safeguards are warranted when it exposes data subjects to adverse decisions. As indicated above, not all data matching does so, but when it does controls are desirable. Data matching involving the collation of data resulting in profiling and adverse decisions thereon is subject to our recommendation at paragraph 11.14 above. Of still greater concern to us 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 programme without data subject consent to justify its need.

11.35 **Our specific recommendations on investigative data matching involving the comparison of data to identify "hits" are as follows:**

Prior approval of the Data Protection Authority 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 supervisory authority shall promulgate mandatory guidelines setting out the relevant factors in determining whether approval shall be granted. These will include the nature and sensitivity of the personal data, its expected accuracy, and the seriousness of consequences of being identified as a "hit". Also relevant is whether it is proposed to inform data subjects in advance.

The guidelines will also set out procedures according "hits" the right to correct matching results before adverse decisions are taken on their basis.

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 that are less satisfactory, and a cost/benefit analysis of the program.

CHAPTER 12

DATA QUALITY AND SECURITY

SUMMARY

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.

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.

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

(i) Personal data should be 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 are accurate records of data received from a data subject or third party and identified as such. (paragraph 12.5)

(ii) Data which are inaccurate or incomplete having regard to the purpose for which it is held, should be erased or rectified. Data should not be kept in a form which permits identification of the data subject any longer than necessary for the fulfilment of the data purposes. (paragraph 12.7)

(iii) 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 12.8)

(iv) 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-

(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. (paragraph 12.25)

DELIBERATIONS

OECD Data Quality Principle

12.1 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."

12.2 To comply with this principle data must be:

- *relevant* to the data to 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, it should be deleted.

- *accurate so* as to adequately reflects the real world. Accuracy is related to the precision of data. The precision required of data will depend on its 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 such other uses as medical records.

- *up-to-date so* that the data reflect the present position.

- *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

12.3 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

12.4 This enactment puts the accuracy requirement succinctly. The 5th principle states:

> *"Personal data shall be accurate and, where necessary, kept up to date."*

12.5 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 such data which are 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 they have previously communicated to them. This is dealt with below. Subject to this, **we recommend adoption of a legal requirement that personal data be accurate and, where necessary, up to date.** Regarding compensation, in Chapter 17 we recommend a general right to compensation for a breach of the legal provisions of the data protection law causing loss. **We further recommend along the lines of the UK legislation, however, that a breach of the accuracy requirement is not compensatable where the data are accurate records of data received from a data subject or third party and identified as such.**

Duty to maintain accurate records

12.6 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

---

1 Fifth Report of the Data Protection Registrar, June 1989, London: HMSO, 1989.

maintain data quality. Data subject correction rights supplement this obligation; they do not qualify it.

Remedying inaccurate records

12.7 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 it is 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 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.

Duty to notify third parties of corrections

12.8 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 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 maintaining 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 notifying a central agency for distribution of corrections as required. In short, it would not be necessary to stipulate the method of propagating correction. 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 it be corrected. This is likely to be facilitated by the tendency to progressively restrict the dissemination of data as its sensitivity increased. While we recognise that it might be objected that the duty may

sometimes be onerous to fulfil, we consider that if a data user chooses to transfer data, the onus should be on him to update it. 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

12.9 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

12.10 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 above that non-automated as well as automated records should be regulated, these include, but are not confined to, computer safeguards. Paper files can be kept under lock and key. Access to computer programs can be user specific or terminal specific. A software application attempts to achieve a similar result. Known as encryption, it involves the scrambling of signals so that they are unintelligible until unscrambled.

The relativity of data security

12.11 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]

---

[2] Bradburn, D "An Introduction to Data Security" in Hearnden (ed.), *A Handbook of Computer Security* (London: Kogan Page, Revised edn; 1990), p.25.

Data security and personal computers

12.12 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. It will be recalled that microcomputers may be linked together into communications networks. The portable nature of microcomputers makes it impracticable requiring 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.

12.13 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.

Intentional computer misuse

12.14 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]

12.15 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]

Computer Crimes Bill 1992

12.16 This Bill was gazetted on 27 March 1992 and is being studied by the Legislative Council. It proposes several amendments to existing laws to counter computer misuse. This discrete approach was adopted in preference to free-standing legislation on the matter. Of particular relevance to the present discussion are clauses 2, 3, and 6. Clause 3 extends the offence of criminal damage to:

---

3 Hearnden, K, "Microcomputer Security" in Hearnden (1990), see note 2, p.150.
4 Hearnden, K, " Computer Security" in Hearnden (1990), see note 2, p.4.
5 Hearnden (1990), see note 2, p.5.

(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.

12.17 A conviction under this provision carries a maximum penalty of 10 years imprisonment. Clause 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." Clause 2 creates the new offence of unauthorised access to a computer by "telecommunication" ie remote means. The maximum penalty provided for is a fine of $20,000.

12.18 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 will screen out innocuous instances.

12.19 Access for gain is dealt with by clause 6 of the Bill. This makes it an offence for a person to obtain access to a computer-

(a) with intent to commit an offence;

(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.

12.20 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 at paragraph 5.35. 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 it for US$175 to private investigators, creditors and businesses.

Computer operating error

12.21 The intentional misuse of computers poses significant security risks to the integrity of personal data. The criminal sanctions contained in the Computer Crimes Bill 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

12.22 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."*

12.23 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 of, personal data and against accidental loss or destruction of personal data."*

12.24 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."*

12.25 We prefer the UK formulation for its clarity, although we would insert "reasonably" before "appropriate steps." It would also have to be made clear that the provision extends to non-automated records. Subject to this, **we recommend its adoption.**

12.26 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

---

[6] Hearnden, K "Computer Linked Crime" in Hearnden (1990), see note 2, p.11

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.

CHAPTER 13

OPENNESS AND DATA PROTECTION

SUMMARY

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.

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.

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

(i) There should be a statutory policy of openness about developments, practices and policies with respect to personal data. The principle should be taken into account:

by the Privacy Commissioner in the carrying out of his functions

by the Data Protection tribunal and the courts

in the formulation and approval of sectoral codes. (paragraph 13.9)

(ii) Users of personal data should compile declarations describing the following features of a personal records system:

- the purposes for which the data are kept
- the content of data contained in the classes of record, including any sensitive content

- the classes of individuals about whom records are kept

- to whom the data are usually disclosed

- the name and address of the person (natural or legal) of the controller of the data, together with the contact details of the individual (the responsible officer) who can provide information to data subjects about access to their personal data. (paragraphs 13.12 and 13.26-27)

(iii) Although a data user is only required to lodge one declaration, separate entries should be made for each functionally separate file or database dealing with a distinct data purpose. (paragraph 13.17)

(iv) For mainstream small business users the declaration will take the form of a structured multi-choice questionnaire. This will accommodate a small number of commonly engaged in data purposes. (paragraph 13.16)

(v) The establishment of a system providing interested individuals with on-fine access to the contents of declarations of organisations. (paragraph 13.24)

DELIBERATIONS

OECD Openness Principle

13.1 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. A GENERAL POLICY OF OPENNESS

13.2 The function of the "general policy of openness about developments, practices and policies" so far as data subjects are concerned is:

> *"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]

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

Openness about new developments

13.3 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.

13.4 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 recommended functions and powers of a data protection agency in Chapter 17.

Legal content of the Openness Principle

13.5 The difficulty of attempting to give legal content to the principle's "general policy of openness" by means other than attributing the relevant function to an oversight authority resides in this very generality. This may explain why many laws based around the data protection principles do not specifically advert to it, although specific provisions may reflect it. So 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

---

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

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.

13.6 The indefinite application of the Openness Principle is largely attributable to it failing 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.

13.7 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?

13.8 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;

(iv) To impose a duty, but on sectors and not individual data users.

13.9 **We recommend on this that 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 it represents a weak freedom of information requirement. The principle**

should be taken into account by the Privacy Commissioner in the carrying out of his functions. Similarly, the Data Protection tribunal 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, but the duty to implement it should not be directly imposed on individual data users. We do not, for example, think it would be a practical requirement of declarations to refer to new administrative or technological developments.

B. MEANS TO ESTABLISH EXISTENCE OF PERSONAL DATA

13.10 The more specific concern of the principle is that mechanisms should exist to facilitate individual data subjects ascertaining what data are held pertaining 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

13.11 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 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 declarations

13.12 To adequately discharge the requirements of both the Purpose Specification Principle and the Openness Principle, **We recommend that declarations describe the following features of a personal records system:**

- **the purposes for which the data are kept**

- **the content of data contained in the classes of record, including any sensitive content**

- **the classes of individuals about whom records are kept**

- **to whom the data are usually disclosed**

- **the name and address of the person (the responsible officer) who can provide information to data subjects about access to their personal data**

- **countries to which personal data are exported to.**

13.13 It might be thought that a declaration entry covering all these matters will be a lengthy document which is time-consuming to compile. This has not been the experience of other jurisdictions imposing a similar requirement. 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.

13.14 A different approach has been adopted under the UK Data Protection Act. As previously mentioned, that legislation 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. The following information on the applicable record keeping purposes is required in the declaration:

- types of individuals about whom data are held

- classes of data held

- sources and disclosures

- overseas transfers

13.15 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, for example. Data users are not confined to the boxes.

13.16 Such a structured form of declaration may be 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.**

Separate entries for each file/database

13.17 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 and relate to a different set of data subjects. It follows that although a data user is only required to lodge one declaration, separate entries should be made for each functionally separate file or database and we so recommend.** 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."*[3]

13.18 The 1989 Australian Digest issued by the Privacy Commissioner further illustrates the point. 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, breathalyzer 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. 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.

---

[3] 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.

Public access to declarations

13.19 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.[4]

13.20 We recommend in Chapter 10 that data users furnish a central authority 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 dialing the relevant telephone code number.

Indexes of declarations

13.21 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[5] 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.

13.22 We find the UK experience instructive in this regard. A central register has been compiled and microfiched copies of the index are available in major public libraries. 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."[6] This is confirmed by the Home Office Review.[7]

13.23 An additional problem identified by Flaherty with digests and central registers which are printed and hence not on-line is that of keeping them up to date.

---

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

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

6 Fifth Report of the Data Protection Registrar, June 1989, London: HMSO, 1989.

7 Home Office, Review of the Data Protection Act Report on Structure, HMSO, 1990.

13.24 **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

13.25 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 sufficient degree of transparency without such a notification requirement that data subjects be notified when data relating to them is first stored.

Appointment of Responsible Officer

13.26 The Openness Principle concludes with the requirement that means should be readily available of establishing the identity and usual residence of the data controller. It is significant that of the three terms that the OECD defines in its guidelines, one is the "data controller". The Explanatory Memorandum refers to it as being:

> *"of vital importance. It attempts to define a subject who, under domestic law, should carry ultimate responsibility for activities concerned with the processing of personal data."*

13.27 The draft Directive similarly defines " controller of the file." As with the OECD definition, it may be a natural or legal person. We discuss the territorial application of the law in Chapter 18 and recommend that the test be control over data processing. We have recommended above that the data controller be identified in the declaration. We also 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 have accordingly recommended above that the contact details of the responsible individual also be included in the declaration.

CHAPTER 14

DATA SUBJECTS RIGHTS OF ACCESS AND CORRECTION

SUMMARY

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.

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".[1] 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

(i) 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 14.9)

(ii) upon receipt of an inquiry as to whether data exist which is unaccompanied by a request of such data, the data user has a discretion as to whether he shall provide a copy of that data. (paragraph 14.9)

(iii) No 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 14.13)

(iv) Access fees should be provided for in subsidiary legislation and in a manner facilitating their updating as required. (paragraph 14.15)

(v) Data access requests should be in a recorded form, although data users may waive this requirement and accept requests by terminals or telephone. (paragraph 14.16)

---

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

(vi) Data provided in response to access requests should 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 of the request when this is in Chinese or English. Where this entails a translation, this should be provided by the data protection authority at a nominal fee. (paragraph 14.17)

(vii) Access requests be responded to within 30 days, in the absence of a reasonable excuse. (paragraph 14.18)

(viii) 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) 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. The reference to information relating to another individual includes a reference to information identifying that individual as the source of information. (paragraphs 14.20-1)

(vii) 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 its use. The log should be available for inspection by the data protection authority and it is also to be provided a periodic return. (paragraphs 14.25-6)

DELIBERATIONS

OECD Individual Participation Principle

14.1 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."

14.2 These access and correction rights are more tersely expressed in article 13 of the draft Directive.

Other jurisdictions

14.3 Data subject access and correction rights are a basic feature of the data protection laws of other jurisdictions. Flaherty points out[2] 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."*[3]

14.4 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[4]. They have since tapered off significantly.

---

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

3 Flaherty (1989), see note 2 above.

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

14.5 Subject access problems constitute a significant proportion of the complaints received by data protection authorities. Of the 1747 complaints received by the UK Data Protection Registrar in 1991/2, 200 related to subject access.[5]

Our earlier recommendations

14.6 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. 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 presently 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.

The mechanics of subject access

14.7 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 its provisions as summarised in the annual reports of the Data Protection Registrar and further evaluated in the Home Office Review.

Material to he provided upon requests

14.8 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

---

5 Eighth Report of the Data Protection Registrar, June 1992, London: HMSO.

as extending to being provided a copy if it does exist, in the absence of any indication to the contrary.

14.9 **We recommend adoption of (a).** As to (b)'s treating an inquiry about data as a request for such data if 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 upon receiving confirmation of being a data subject. Also, ascertaining whether data are held on an individual will usually make it a simple matter to have it 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 of such data, the data user has a discretion as to whether he shall provide a copy of that data.**

Provision of description of data purposes

14.10 The Home Office Review recommends (following the Registrar's 1989 review) that in addition to the present requirements of confirmation of whether the applicant is a data subject and if so an intelligible copy of any such data, there should be supplied:

(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

14.11 The Home Office Review concludes that data purposes are the matter most likely to be of concern to a data subject. A perusal of data purposes as set out in an organisations's declaration would accordingly 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 obtain a copy of data held, it would save data users from having to provide a copy of any data held in response to every inquiry. We have recommended in Chapter 13 that data users compile declarations which would include items (i) and (ii). We also agree that its contents are relevant both to the individual's decision whether to make a request of 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 it deters them from initially following the matter up with the data user.

Fees

14.12 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.

14.13 **We recommend that no fee be payable by a data subject merely inquiring as to whether data exist relating to him. A fee should be payable for full access requests which require the supply of a copy of data held, to deter mischievous requests. 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.

14.14 Where the data user has separate entries in his declaration concerning different databases with different purposes, the issue arises whether the data subject should be charged a separate fee for a copy of the data from each database. He will not usually be able to do so in advance, as he will not know how many entries relate to him. 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?

14.15 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, its insertion in a bylaw would facilitate the updating of fees as required. **We recommend that the question of fees be provided for in subsidiary legislation.**

Form of request

14.16 The question arises of the form of a request by an individual that an organisation confirm whether it holds data on him and, if so, 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

14.17 **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. As Hong Kong is a multilingual society, we further recommend that data users should respond in the language of the 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.** We consider it necessary to involve the authority in the translation process because he will possess the expertise required to provide the technical format necessary to satisfy the intelligibility requirement.

Time limits

14.18 **We recommend the imposition of a requirement that access requests be responded to within 30 days, in the absence of a reasonable excuse.** Determining the reasonableness of the excuse would ultimately be a matter for the data protection authority.

Limitations on data access

14.19 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."

14.20 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. It is not made 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 included in Hong Kong.**

14.21 We also agree with the general aim of section 21(4)(b). Its operation is extended 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 recommend that these provisions be adopted also.**

14.22 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.

Exemptions to data access

14.23 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

14.24 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."*[6]

14.25 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.

14.26 The Registrar's recommendation would appear to provide a useful check on the claiming of exemptions, but we are not sure if his 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**

---

6 Fifth Report of the Data Protection Registrar, June 1989, London: HMSO.

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.

CHAPTER 15

EXEMPTIONS

SUMMARY

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.

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.

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.

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.

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]

The discussion in this chapter is concerned with the exemptions to be included in the principal data protection legislation. Other ordinances

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

will also effect partial exemptions and chapter 3 examined the legislation that may partially overlap the operation of a data protection ordinance.

RECOMMENDATIONS

(i) 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 15.6)

(ii) Non-profit making bodies should be exempted from the obligation to furnish a copy of their declaration to the data protection authority, provided the data relate only to their members and is not communicated to third parties recreational purposes. (paragraph 15.7)

(iii) Data held for the purpose of national security, defence, and international relations should be completely exempted from subject access and from the non-disclosure provisions recommended in earlier chapters. A certificate signed by the Governor would be evidence of the exemption. Data users should nonetheless remain subject to the general requirement of furnishing declarations describing data held for these purposes. Also, the other data protection principles should apply. The Privacy Commissioner should not, however, be entitled to monitor compliance with the remaining data protection principles. His role should be restricted to being entitled to look behind the Governor's certificate to confirm that the data purpose for which the exemption was claimed is correctly classified. (paragraph 15.18)

(iv) A complaints mechanism along the lines of the UK Security Service Act 1989 should be adopted regarding the activities of the security service. (paragraph 15.19)

(v) Personal data should be exempted whose disclosure is urgently required for preventing serious injury or other damage to the health of any person or persons should be exempted from the application of provisions limiting its disclosure to third parties. (paragraph 15.23)

(vi) Personal data held for the purposes of-

> *"(a) the prevention or detection of crime;*
>
> *(b) the apprehension or prosecution of offenders; or*
>
> *(c) the assessment or collection of any tax or duty,*

should be exempt from the subject access and non-disclosure provisions in any case in which the application of the those provisions would be likely to prejudice those purposes." (paragraph 15.24)

(vii) The Council of Europe recommendations regulating the use of personal data in the police sector should be adopted. (paragraph 15.26)

(viii) An exemption from the access provisions recommended in the last chapter should be provided for:

(a) evaluative material or other data pertaining to appointments particularly affecting the public interest, such as to the judiciary and regulators of the financial markets. (paragraph 15.36)

(b) data for which a claim for legal professional privilege could be made out. (paragraph 15.37)

(c) data of such a nature that providing access is likely to cause serious harm to the physical or mental health of the data subject. (paragraph 15.39)

(ix) Where an exemption from the access provisions is provided for competing public purposes, access requests should be complied with insofar as it is possible to do so without prejudicing those purposes. (paragraph 15.40) Furthermore, with the exception of access exemptions claimed for national security, defence or international relations (as to which see (iii) above), the data protection authority should upon application review the release of data where the data user has claimed an access exemption. (paragraph 15.42)

DELIBERATIONS

A. DATA PURPOSES WITH LIMITED PRIVACY IMPLICATIONS

Data used solely for private and personal purposes

15.1 Article 2 of the ECC 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 UK 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."*

15.2 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 relating to the data subject. They are also likely to participate in the exchange of personal data.

15.3 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 disclosed a copy of the list or letter to a government department or company, he would no longer be able to claim the exemption.

Earlier recommendations

15.4 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

15.5 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, it will only influence the individual's perception of the data subject, if kept solely for his personal purposes. 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 Bill of Rights Ordinance (Cap 383) ("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 at paragraph 15.28 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

15.6 **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

15.7 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. In Hong Kong so-called "clubs" are both endemic and problematic. The position is complicated by the Societies Ordinance (Cap 151) as amended by the Societies (Amendment) Ordinance 1992. Also, a distinction needs to be drawn between non-profit-making bodies and bodies whose purposes are not specifically to make profits but are nonetheless profitable. An example of the latter is the Royal Hong Kong Jockey Club, an organisation which holds detailed personal data on its many members. The records of such bodies have the potential to be misused. On the other hand, we wish to avoid imposing unnecessary administrative requirements on small organisations. To safeguard members, however, the data protection principles should apply to all organisations. It is difficult to draw the line but certainly as regards unincorporated associations not conducting a business and without employees we think an administrative concession is warranted. Such bodies should compile a declaration available for inspection by members. But **we**

recommend they be exempted from the obligation to furnish a copy of their declaration to the data protection authority, provided the data relates only to their members and is not communicated to third parties.

Other data purposes arguably not infringing privacy

15.8 The UK Act also completely exempts personal data held solely for 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

15.9 Some data protection laws completely exempt publications and public registers. The difficulty with this is that it sanctions data collected for one purpose being used for another purpose not originally envisaged by the person furnishing the data. On the other hand, the nature of a particular publication may obviously envisage a variety of purposes. We consider that publications and public registers should be subject to the general application of the data protection principles. More specific restrictions on their use should be included in the relevant legislation (eg Hong Kong electoral roles are not public documents).

B. PUBLIC INTEREST EXEMPTIONS

15.10 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

15.11 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 UK 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 principle

---

2 Fifth Report of the Data Protection Registrar, June 1989, London: HMSO, 1989.

limiting disclosure (the OECD equivalent is the Use Limitation Principle) and that 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.

15.12 Whilst we broadly agree with the structure of the UK 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 UK equivalent) will now be briefly reviewed.

Exemptions and the Bill of Rights

15.13 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 International Covenant on Civil and Political Rights. 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;

(iii) request rectification or elimination of incorrect personal data.

15.14 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* [1992] 1 HKCLR 127 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* ((1987) 9 EHRR 433) 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.

15.15 Against this background we now examine data purposes involving dominant social interests meriting exemptions from a data protection law. The UK Act will be referred to as a basis for discussion.

National security

15.16 Section 27 of the UK 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."

15.17 The following aspects of this provision require comment:

(i) Lack of definition

"National security" is undefined in the legislation. While it is also undefined in s.1 (2) of the UK 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. This is relevant to the issue of the appropriate width of the exemption to be provided under this head.

(ii) Impact on ordinary individuals

Related to the possible width of "national security" is the potential for the purpose to impinge on ordinary individuals. UK security vetting figures 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).[3]

(iii) Scope of the exemption

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 UK Act, only registered data users are subject to an enforceable duty to comply with the principles.

(iv) Exemption relates to data purpose

In common with the other exemptions under the UK Act, 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.

(v) Supplementary legislative protection

Although individuals are denied any redress under the 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 M15, the UK's domestic security service. An individual's career may be ruined, for example, by a misinformed vetting assessment. The Act establishes a tribunal of lawyers to investigate complaints. It follows that in the UK security service outsiders are now conferred a general supervisory role. They do not, however, possess a monitoring role in relation to the application of the data protection principles to the collection and use of security-related data.

Recommendations on data held for national security purposes

15.18 At paragraph 15.40 below, we endorse as a general principle indirect data access through a data protection authority. In the Hong Kong context this may not be feasible for national security data. In this category we also put international relations and defence, as these interests will often overlap in practice. We note that the three interests are all explicitly addressed in the Official Secrets Act 1989. On the other hand, the UK Data Protection Act only purports to exempt "national security". This could be attributable to "defence" and "international relations" being readily subsumable under the broad rubric of "national security." Given the vagueness of that last expression, expressly adding the other two purposes may not be effectively broadening the scope of the exemption. **We**

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

recommend that data held for the purpose of national security, defence, and international relations should be completely exempted from the subject access and non-disclosure provisions recommended in earlier chapters. A certificate signed by the Governor would be evidence of the exemption. Data users would nonetheless remain subject to the general requirement of furnishing declarations describing systems holding data for these purposes. Also, the other data protection principles would apply. The Privacy Commissioner would not, however, be entitled to monitor compliance with the remaining data protection principles. His role would be restricted to being entitled to look behind the Governor's certificate to confirm that the data purpose for which the exemption was claimed was correctly classified. This latter feature goes further than the UK provision, and is thought necessary in view of the matters raised at paragraphs 5.13-17.

15.19 In addition, **we recommend the adoption of a complaints mechanism regarding the activities of the security service along the lines of the UK Security Service Act 1989.** This is to provide an element of independent monitoring, in view of BOR requirements. As that legislation does not provide for the independent scrutiny of security service databases, it is not completely clear whether this will satisfy the BOR. These doubts will disappear in relation to national security data if indirect access were provided through the data protection authority. This is discussed at paragraph 15.39 below.

The media

15.20 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 on possible abuses. The difficulty is determining where to draw the line between the exercise of freedom of expression and the potentially competing right to privacy. Article 9 of the draft Directive addresses the issue in the following terms:

> *"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."*

15.21 The accompanying Explanatory Memorandum explains that in determining the appropriate scope of such an exemption, relevant considerations include the availability of administrative or legal remedies, including a right of reply, the existence of a code of professional ethics, and the terms of the relevant human rights documents.

15.22 We will be reviewing these matters when we examine the media and privacy in a subsequent document. Only then will we be equipped to

make recommendations on the precise extent to which the media should be exempted from data protection requirements.

Public health and safety

15.23 Section 34(8) of the UK Data protection Act exempts from the non-disclosure provisions 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 provision in Hong Kong, subject to it being limited to "serious" injury.**

Crime and taxation

15.24 Section 28 of the UK Act provides that personal data held for the purposes of-

> *"(a) the prevention or detection of crime;*
>
> *(b) the apprehension or prosecution of offenders; or*
>
> *(c) the assessment or collection of any tax or duty,"*

are exempt from the subject access and non-disclosure provisions "in any case in which the application of the those provisions would be likely to prejudice" those purposes. Again, 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 relate to (a) or (b). Personnel records would not, for example. Further, as with all exemptions under the UK Act except national security, data exempted from these two data protection principles are subject to the other principles, and to registration requirements precluding secret databases.

COE recommendations on police data

15.25 The Council of Europe has promulgated a detailed set of recommendations regulating the use of personal data in the police sector[4]. 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.

---

[4] Council Of Europe, *Regulating the Use of Personal data in the Police Sector*, (Strasbourg 1988)

Recommendations on exemptions for law enforcement and tax

15.26 **We recommend non-disclosure and access exemptions for law enforcement and taxation purposes along UK lines, subject to our general comments at paragraph 15.40 below on indirect access. We further recommend adoption of the Council of Europe recommendations regulating the use of personal data in the police sector.**

C. EXEMPTION OF CONFIDENTIAL DATA

Confidentiality and access

15.27 The common law duty of confidence was discussed at Chapter 4 above. It will be recalled that a legally enforceable duty limits the disclosure of information not publicly known and entrusted to a person in circumstances imposing a duty of confidence. We commented on the doctrine's similar content to the Use Limitation principle. We concluded that with its rather different scope of application, it complements the protection to personal information provided by the Purpose Limitation Principle.

15.28 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."*[5]

15.29 Access rights under a data protection law constitute such a statutory authorisation 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.

15.30 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

---

5 Wacks, R, *Personal Information: Privacy and the Law* (Oxford, Clarendon Press, 1989), p.78.

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 recommend below detailed access exemptions where confidentiality is buttressed by additional public interest considerations. But we reject a general exemption to subject access rights which focuses on the conditions of its transfer to the data user, namely that it was provided "in confidence".

Confidential data with additional public interest aspects

15.31 The following are examples of data which will usually have been provided in confidence, but for which additional public interest grounds exist justifying exemption from data access requirements.

Supervision of financial markets

15.32 The supervision of the financial markets entails ensuring that people of doubtful integrity are not allowed to run businesses entrusted with the public's savings and investments. The candid exchange of personal information among the international network of supervisors is vital in determining the fitness of office holders of such businesses. Such information is usually provided subject to its confidentiality being respected. Section 30 of the UK Act accordingly exempts such data from the access provisions where it would prejudice this purpose.

Judicial appointments

15.33 Another category of appointments singled out by the UK Act is that of the judiciary. Section 31(1) exempts from the access provisions data received from third parties relevant to the making of judicial appointments.

A general access exemption for testimonials?

15.34 The UK Act's access exemptions regarding data relevant to appointments is restricted to those in the financial markets and the judiciary. An alternative approach which avoids the difficult legislative task of singling out important appointments is a general exemption for references. This approach is taken in the New Zealand Privacy of Information Bill. Clause 28(b) of the Bill exempts from access "evaluative" material (presumably excluding purely factual data) provided in confidence compiled solely for the purposes of determining the suitability of an individual for employment.

15.35 We note that the UK law's lack of a general exemption for testimonials does not appear to have caused any problems. We do not,

however, find it an easy issue. We recognise that individuals could feel inhibited in providing candid assessments if aware that access may be granted. On the other hand, we are concerned that recorded assessments may be erroneous or unfair and result in long term damage to the data subject's prospects. Access rights facilitate the correction of errors. There is the additional argument that people will be less prone to make sweeping assessments if aware that they may be scrutinised. We accordingly do not recommend a general exemption for testimonials from the access requirements of the law. We do not consider that this will unduly inhibit everyday administration. First, it will remain possible for referees to furnish confidential testimonials denying access rights with the informed consent of the data subject. Second, it will not affect oral assessments which are not reduced to recorded data, as the access rights would have nothing to fix onto.

15.36 We agree, however, that there is a public interest in ensuring that certain positions are properly filled. The public interest would be particularly adversely affected by unsuitable appointments in the two spheres identified by the UK Act, namely the regulation of the financial markets and the judiciary. There may well be others, however. **We accordingly recommend an exemption to access regarding evaluative material or other data pertaining to appointments particularly affecting the public interest.**

Legal professional privilege

15.37 Legal professional privilege is the legal principle whereby communications made to and from a legal adviser are protected from disclosure in the course of legal proceedings. It 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 by other professional relationships reflects the singular importance that the common law attaches to ensuring the unrestricted communication between parties and their legal advisers. The UK legislature has taken a similar view in section 31(2) of the UK Act. **We recommend an exemption from the access provisions data for which a claim for legal professional privilege could be made out.**

Confidential health and social work data

15.38 Section 29 of the UK Act provides that the Secretary of State may by order exempt from or modify the application of the access provisions regarding social work data or data subject's physical or mental health. Orders have since been made dealing with all these areas. The UK legislature has also recognised that data of this description is held manually as well as in the computerised form envisaged by the Data Protection Act. It has accordingly also enacted supplementary legislation covering manually held records in these areas, although there are some discrepancies between

their provisions and those in the Data Protection Act. (Our earlier recommendation that data be regulated regardless of the storage medium aims at avoiding these problems.) The main thrust of both sets of provisions, however, is 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 paragraph 4.30 above).

15.39 We agree with the rationale of the first limb of the UK 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 it is likely to cause serious harm to the physical or mental health of the data subject.** We have reservations, however, about according social welfare informants the same protection from access as police informants. We think that the recommendations below regarding access exemptions should cover the field, namely those regarding the prevention of crime and of serious injury. We do not recommend that this aspect of the UK legislation be adopted here.

15.40 A further difficulty is that the statutory language could suggest that an all-or-nothing approach is warranted. But as we commented regarding a similar problem dealt with at paragraph 14.20 above, judicious editing by the data user will often facilitate release of most if not all of the data which are the subject of the request. **We 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 competing public purpose.**

Indirect access through data protection authority

15.41 A general deficiency of the UK access exemptions is that the data user is the sole arbiter of whether providing access is likely to prejudice the purpose in question. This is only subject to appeal to a court. We consider this too inflexible and prefer the system adopted in a number of European jurisdictions 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 15 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 checks, at the data subject's request, so as to verify the lawfulness of the processing within the meaning of this Directive."

15.42 We endorse this mechanism of indirect access. The independent review of the release of security and police data are viewed in France and Germany as an important protection of civil liberties. In our recommendation above on national security data we have not recommended any oversight role for the data protection authority, other than to verify that it does relate to the purpose claimed. But this special case aside, we consider indirect access as a necessary control mechanism of general application to all access exemptions. **We therefore recommend that except in the case of data held for national security, defence or international relations purposes, the data protection authority shall upon application review the release of data where the data user has claimed an access exemption.**

CHAPTER 16

STRUCTURE AND POWERS OF ENFORCEMENT AGENCY

SUMMARY

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 of enforcement be established. Most countries with data protection laws have established such bodies.

Investigation of complaints by an enforcement agency assists data subjects to enforce their rights and means that litigation need only be resorted to for appeals or judicial review.

This chapter examines the structure appropriate for the enforcement authority. We think the chief executive should have an investigative role and be assisted in policy formulation by a board.

We consider the independence of the authority 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.

RECOMMENDATIONS

(i) Overseeing compliance with the regulatory requirements of a data protection law should be the sole responsibility of an independent agency established for the purpose. In addition to assisting individuals to enforce their rights, the agency 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. (paragraphs 16.7-8)

(ii) The data protection oversight authority should comprise a board of commissioners to be chaired by a full-time Privacy Commissioner. He should be assisted in the formulation of policy by the following part-time members:

(a) one member with high level experience in the public sector and one member with equivalent experience in the private sector.

We recognise that this distinction is not always easy to draw (eg hospitals or tertiary institutions) and this point is accommodated by (iv).

(b) one member with extensive experience in data processing (information management) and one member with similar experience in records management.

(c) two members to represent general community interests.

(d) three members with general experience. (paragraph 16.11)

(iii) The Privacy Commissioner and the commissioners should be appointed by the Governor on the advice of the President of the Legislative Council. 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 16.13)

(iv) The tenure of the Privacy Commissioner and the commissioners should be protected by a provision requiring that they 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. (paragraph 16.14)

(v) A majority of the part-time commissioners should not be public officers. The Board should meet not less than quarterly. (paragraph 16.12)

(vi) To secure an adequate budget, a levy of $100 should be levied on all applicants for business registration. (paragraph 16.17)

DELIBERATIONS

The need for an independent enforcement agency

16.1 In only one country is the enforcement of the data protection principles left to the data subject, unaided by an enforcement agency. 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. Also, delays commonly characterise the conduct of litigation and figures indicate that this is true of US privacy claims.[1]

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

16.2 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 the infringement of it. 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. But whilst such provision may be useful if used in moderation to supplement an enforcement regime, we consider that sole reliance on civil remedies affords data subjects inadequate protection.

16.3 In addition to assisting data subjects to uphold their privacy rights, effective enforcement of a data protection regime requires a government agency to exercise a general monitoring role. As mentioned above, 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 enforcement requires a truly independent agency specifically charged with this task.

International instruments on need for independent agency

16.4 International instruments dealing with data protection have recently specifically addressed the need for a supervisory authority. Article 30(1) of the European Communities Commission 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."*

16.5 It will be recalled from Chapter 4 that the terms of the Hong Kong Bill of Rights (Cap 383) ("the BOR") are based on those of the International Covenant on Civil and Political Rights ("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 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 it. They would accordingly constitute persuasive authority

---

[2] Flaherty (1989), see note 1 above.

regarding 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

16.6 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 latter has been mooted in Hong Kong, following the enactment of the BOR. The provisions of that legislation 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 an enforcement agency would have a far more specific role than one of overseeing the BOR generally. The latter option accordingly raises different considerations and we express no opinion on it, it being outside our terms of reference.

Recommendation on independent authority

16.7 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 agency tasked to monitor compliance with the regulatory framework proposed above.** In addition to assisting individuals to enforce their rights, the agency 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 in the next chapter.

Sole responsibility for overseeing data protection

16.8 Agencies 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 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 enforcement agency be fully responsible for the implementation of a data protection regime in Hong Kong.**

Structure of the authority

16.9 There is less agreement among other jurisdictions on whether the chief executive should be assisted by a board of advisors or commissioners. (For convenience, we shall refer to the Chief Executive as the "Privacy Commissioner", but this will not preclude the adoption of a more apt title expressing the functions of the enforcement agency once these have been clarified in the second part of this law reform reference). 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.

Board of commissioners

16.10 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 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. This will also avoid liaison problems.

---

[3] Flaherty (1989), see note 1 above, p.250

16.11 **We therefore recommend the establishment of a board of part-time commissioners to be chaired by the Privacy Commissioner and comprising the following:**

(i) one member with high level experience in the public sector and one member with equivalent experience in the private sector. We recognise that this distinction is not always easy to draw (eg hospitals or tertiary institutions) and this point is accommodated by (iv).

(ii) one member with extensive experience in data processing (information management) and one member with similar experience in records management.

(iii) two members to represent general community interests.

(iv) three members with general experience.

16.12 A board of nine members is accordingly recommended to assist the Privacy Commissioner in policy formulation. This number provides a variety of perspectives without being unwieldy. **We further recommend that a majority not be public officers, to avoid domination by the Executive. 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.

Independence

16.13 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. **We accordingly recommend that the Privacy Commissioner and the commissioners be appointed by the Governor on the advice of the President of the Legislative Council. 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.**

16.14 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 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 and the commissioners.

Adequate budget

16.15 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 of course 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 Federal electronic data processing.[5]

The cost of data protection regulation

16.16 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 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.

Business registration levy

16.17 In earlier chapters 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 300,000 registered businesses in Hong Kong. The current annual registration fee is $1,150. 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.

---

4 Flaherty (1989), see note 1 above, p.55.

5 Flaherty (1989), see note 1 above, p.42.

CHAPTER 17

FUNCTIONS AND POWERS OF THE DATA PROTECTION AGENCY

SUMMARY

This chapter examines the functions which a data protection authority should perform. We believe that the authority should not be restricted to responding to complaints but should be able to initiate its own investigations and on-site inspections.

Data users will have to provide the declarations described in previous chapters to the authority. The authority will establish sectoral codes of conduct and publicise data protection requirements.

The chapter looks at the powers necessary to enable the authority to carry out its functions. We believe that powers to enter premises and obtain evidence are necessary. 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.

We consider that a specialised tribunal should be established to determine the merits of disputes between data subjects and data users as we believe that the courts are not well equipped to consider such disputes.

RECOMMENDATIONS

(i) The data protection authority ("the Privacy Commissioner") should have the following functions:

(a) investigation of complaints

(b) the conduct of on-site inspections of record keepers

(c) notification point for declarations from data users

(d) promoting codes of conduct

(e) educational and publicity functions. (paragraph 17.1)

(ii) 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 17.4)

(iii) The Privacy Commissioner should have a limited discretion to decline to investigate complaints on well-established grounds regarding lack of merit. (paragraph 17.4)

(iv) Data subjects should have the right to complain direct to the Privacy Commissioner. (paragraph 17.6)

(v) 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 17.7)

(vi) 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 2 or more individuals, any one of those individuals may make a complaint. (paragraph 17.8)

(vii) The Privacy Commissioner should be conferred 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 may hear or obtain information from such persons, and make such inquiries, as he thinks fit. A person shall only be entitled to be heard by the Commissioner if the Commissioner is proposing to make an adverse report or recommendation on him. (paragraph 17.9)

(viii) When a hearing is necessary, it should be held in public unless one of the parties requests otherwise, in which case the hearing should be in private. (paragraph 17.11)

(x) In the course of such hearings, 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 17.12)

(x) 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 17.13)

(xi) Data subjects may judicially review but should not have the right to have reviewed on its merits the decision of the Privacy Commissioner not to investigate a complaint or not to take enforcement action following an investigation. (paragraph 17.14)

(xii) The Privacy Commissioner should be expressly empowered to conduct investigations in the absence of a complaint, provided he has reasonable grounds for suspecting a breach of the principles. This would be

additional to the duty to investigate complaints received from data subjects, or referred to him by the board of commissioners. (paragraph 17.16)

(xiii) 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 17.17)

(xiv) A right to compensation should accrue from any breach of the data protection principles causing loss and injured feelings, including injured feelings unaccompanied by loss. (paragraph 17.20) The Privacy Commissioner's role in compensation claims should be limited to determining whether there had 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 17.21)

(xv) 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 17.25) It should be expressly provided that the power be exercised in a manner that does not unduly disrupt daily operations. (paragraph 17.26)

(xvi) The Privacy Commissioner and his staff should be subject to a legal duty of secrecy subject to criminal sanctions. (paragraph 17.27)

(xvii) 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 17.31)

(xviii) Sectoral codes of conduct 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 should it be necessary to determine whether there had been a breach of the principles. (paragraph 17.33)

(xix) 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, he should initially approach the organisation's officer responsible for data protection matters ("the 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 17.37)

(b) where entry is urgent, he should initially seek the consent of the Responsible Officer, but if it is declined the Commissioner should approach the court forthwith, thereby dispensing with the 14 day grace period. Where the Commissioner considers it inadvisable to alert the organisation to his imminent visit (eg to avoid the destruction of evidence) 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 17.38)

(xx) The Privacy Commissioner should be empowered to serve notice on any person requiring him to furnish in writing such information (on oath, if the Privacy Commissioner thinks fit) or to produce any document or thing as is necessary or expedient for the performance of his 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 17.39)

(xxi) 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 Ordinance has been contravened in respect of some of its contents and that exempt data are returned within a reasonable period. (paragraph 17.40)

(xxii) It should be a criminal offence to wilfully make a false statement to the Privacy Commissioner, the offence not being tied to requirement that evidence be given on oath. (paragraph 17.41)

(xxiii) The Privacy Commissioner's decisions should be subject to judicial review. (paragraph 17.42) 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 a specially constituted tribunal and not a court. The Tribunal should consist of three part-time members and be chaired by a legally qualified person. The Chairman should be assisted by a member experienced in information management and the third member should be a layman. Members should be appointed for three years, with the option of one reappointment. The hearing before the tribunal should not be a full rehearing, but restricted to a review of the correctness of the decision appealed from in the light of the

evidence below, together with any new evidence or explanations provided by either party at the appeal hearing. Parties should have the legal right to appear in person and, at the discretion of the Tribunal, through counsel. Evidence should be on oath. The Tribunal should have the power to award costs. It should give written reasons for its decisions. There should be a right of appeal from the Tribunal to a court on questions of law only. (paragraph 17.42)

DELIBERATIONS

A. FUNCTIONS OF A DATA PROTECTION AUTHORITY

17.1 **We recommend that the data protection authority have the following functions:**

(i) investigation of complaints

(ii) the conduct of on-site inspections of record keepers

(iii) notification point for declarations from data users

(iv) promoting codes of conduct

(v) educational and publicity functions.

17.2 Before examining these functions in detail, a general point may be in order. The UK Act fails to specifically identify all the Registrar's various functions. It is subsumed under the very general ambit of section 36(1). This simply provides that "it shall be the duty of the Registrar so to perform his functions under this Act as to promote the observance of the data protection principles." So, for example, the Registrar rightly attaches great importance to education and publicity, but the legislation omits express reference to this function. 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.

1. INVESTIGATION OF COMPLAINTS

17.3 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 1747 complaints, down from the previous year's 2419. 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%).[1] The Australian Act covers a much smaller population and focuses on the public

[1] Eighth Report of the Data Protection Registrar, June 1992, London: HMSO.

sector. For the year ending June 1991 the Australian Privacy Commissioner received 66 complaints falling within his jurisdiction. The most frequently cited processing complaint related to limits on use and disclosure, followed by storage and access, collection, accuracy and use of data.

Scope of duty to consider complaints

17.4 The subject matter of complaints should be widely drawn. So 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 complaints "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 locally 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.**

False complaints

17.5 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.

Direct access

17.6 The comparatively specialised nature of data protection requires that data subjects should have direct access to the enforcement agency. A referral system such as has hitherto been in place for the Commissioner of Administrative Complaints would be unworkable in this area. We note that in any event there is now to be direct access to the Commissioner. There is direct access to the UK Data Protection Registrar. **We accordingly recommend that data subjects have the right to complain direct to the Privacy Commissioner.**

Form of complaints

17.7 **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 is not contained in the UK Act, but is provided for in the Australian Act, for example.

Class complaints

17.8 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 …"**

Procedure for hearing data subject complaints

17.9 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) provides that "he 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 taciturn on procedural matters. We prefer the more explicit approach and **we**

recommend adoption, suitably adapted, of the procedural provisions of Cap 397.

17.10 If these recommendations are adopted, the Privacy Commissioner will share the flexibility his or her overseas counterparts enjoy in adopting as informal 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.

Private hearings

17.11 A related point is that either the complainant or respondent will often wish the hearing to be in private. We think such requests should be deferred to. The very notion of a "privacy hearing" is indeed slightly contradictory. We are also conscious, however, that the lack of public scrutiny afforded by private hearings could occasion concern for potential official abuse. **We therefore recommend that hearings be held in public unless one of the parties requests otherwise, in which case the hearing should be in private.**

Legal representation

17.12 **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.**

Disposal of complaints

17.13 **We recommend the 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.

17.14 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 on this that data subjects should not have the right to have reviewed on its merits non-action by the Privacy Commissioner.** We think that judicial review provides an adequate oversight mechanism in this regard. Also, 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 making initial inquiries.

Investigations without complaints

17.15 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 to those complaints which the Registrar has a duty to consider."[2]. 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 of a contravention of the data protection principles. So 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 appropriate for him conduct a thorough on-site inspection.

Commissioner of Administrative Complaints distinguished

17.16 In the Hong Kong context, the Commissioner of Administrative Complaints performs a somewhat analogous ombudsman role to that envisaged for the Privacy Commissioner, in that he investigates complaints, albeit of a more general nature. The legislation restricts him to a reactive role, as he may only conduct investigations in response to complaints. He is not empowered to investigate, even upon reasonable grounds, a matter at his

---

2 Fifth Report of the Data Protection Registrar, June 1989, London: HMSO, para 199.

own initiative. We think a more proactive role is required as regards data protection. Data protection regulation requires a flexible approach. The data protection principles are abstract and open-textured. Furthermore, the Privacy Commissioner's vantage point will often apprise him of matters which data subjects will be unaware of. **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 principles. This would be additional to the duty to investigate complaints received from data subjects, or referred to him by the board of commissioners.**

Remedies for substantiated complaints

17.17 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 users'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 from processing personal data. A similar power is 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 an order is warranted.**

Compensation for complainants

17.18 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."

17.19 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 acts commonly provide for the payment of compensation, but the scope of such provisions vary. Some data protection acts (the Australian Act is an example) provide that compensation may accrue from any breach of the principles. The UK Act is considerably more restrictive, limiting compensation claims to those involving data inaccuracy, destruction, or unauthorised disclosure. The UK Registrar has recommended that this be changed and that the Registrar be empowered to direct compensation up to 5000 pounds for damage and associated distress arising from any breach of the principles[3]. 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."[4]

17.20 These are relevant considerations, although the Home Office concedes that they involve an element of speculation, no compensation claims having 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 4 years, she could not recall any involving a significant compensation claim. More fundamentally, however, we can see no basis in principle for 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 and injured feelings, including injured feelings unaccompanied by loss. (Chapter 12 recommends that inaccurate data not be compensatable if an accurate record of data received and identified as such.)** 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

---

3 Fifth Report of the Data Protection Registrar, June 1989, London: HMSO, para 214.

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

injured feelings (*AG v. Guardian Newspapers Ltd* (No 2) 3 All ER 545 at p.639). It will, in any event, be for the court to determine quantum.

Appropriate body to determine compensation

17.21 The remaining question is 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 had 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. Also, as claims are likely to be for comparatively small amounts, they will often fall within the jurisdiction of the Small Claims Tribunal.

2. ON-SITE INSPECTIONS

17.22 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 enforcement agency. The Australian Act provides the Privacy Commissioner with the power to conduct audits of personal records and has referred to it 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 [5]. 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 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

---

[5] Flaherty, David, *Protecting Privacy in Surveillance Societies* (University of North Carolina Press, 1989), p.343.

usually have backgrounds in data processing rather than law to equip them to ask technical questions, such as what defence strategies are taken against intrusive measures.

17.23 The above 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 be caused to the activities of inspected organisations. Banks 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.

17.24 We note that the UK law does not presently possess 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."[6] 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.

17.25 In view of the above **we recommend that the Privacy Commissioner have the power to initiate systematic inspections of personal data 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 declaration description of data purposes, classes of data subjects etc. 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 properly conduct their data processing.

17.26 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 daily operations.**

---

6 Fifth Report of the Data Protection Registrar, June 1989, London: HMSO, para 206.

Inspections and secrecy

17.27 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 agency staff on the same footing as other officials dealing with confidential information, such as those employed by the Taxation Office (see paragraph 3.4 above). It would extend beyond inspections and encompass all information acquired in the course of duties, be it personal data or trade secrets.

3. ADMINISTRATION OF DECLARATION SYSTEM

Declarations and the data protection principles

17.28 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 would briefly describe record purposes, contents of records, classes of data subjects, classes of transferees, countries to whom data export was proposed, and contact details of the organisation's Responsible Officer. 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 facilitate data subjects ascertaining 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.

Declarations and the functions of the agency

17.29 In addition to facilitating the implementation of the data protection principles, commentators attribute several other benefits to a declaration system. Its compilation 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 it is a standard requirement that it be furnished with a copy. This requirement (which we recommend above) enables the agency to maintain a true oversight role. It also provides it with a list of data users. It 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 point of departure in the conduct of such inspections. Policy formulation should also benefit.

Avoidance of bureaucracy

17.30 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. 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. But those two jurisdictions require not only that data users furnish the authority with a declaration, but that the authority has a duty to decide whether to accept or reject the proposed data uses. This is also the UK position.

17.31 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 is not 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.

4. CODES OF CONDUCT

17.32 Reference is frequently made in data protection to "self-regulation within the law." This report recommends a detailed regulatory scheme applying to all data users, unless one of the exemptions discussed in chapter 15 applies. We recognise, however, that data uses do differ between sectors. The data protection principles are flexible enough to accommodate this. For example, data purposes differ between sectors and the Purpose Limitation Principle acknowledges this. We agree with the UK Registrar's following 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."[7]

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

17.34 Notwithstanding the limited legal scope of sectoral codes, we wish to emphasise 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 provides flexibility, codes can usefully furnish more specific guidance by elaborating on the principles.

5. EDUCATION AND PUBLICITY

17.35 Perhaps the single greatest obstacle to the implementation of data protection is lack of knowledge by the ordinary data user. The importance of this function 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 subjects." 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.

---

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

B. POWERS OF THE PRIVACY COMMISSIONER

Introduction

17.36 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

17.37 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 authorisation, 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 its absence. **We accordingly recommend that with those cases that the Privacy Commissioner considers not urgent, he should initially approach the organisation's officer responsible for data protection matters. 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

17.38 This comparatively protracted procedure is obviously inappropriate for urgent cases, such as where large-scale transborder data exports are feared imminent. **We recommend the following procedure where urgent entry is necessary; if the Responsible Officer declines consent at the outset, the Commissioner would approach the court forthwith, thereby dispensing with the 14 day grace period. There will be other cases where 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 lines 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* [1976] 1 All ER 799. That decision upheld the validity of the procedure whereby a court order may be applied for

against an absent party. Commonly used in copyright proceedings, it would be invoked when alerting the other party to the proceedings is likely to result in the disappearance of the infringing materials.

Evidence

17.39 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 require supplementing, however, by obtaining 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 presently 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 Netherlands (section 45). Locally, Cap 397 confers substantial powers on the Commissioner of Administrative Complaints in this regard. It is not limited to information in writing, encompassing a requirement to furnish the Commissioner "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.**

Exempt data

17.40 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 firstly necessary to examine the data to ascertain whether it is 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 is returned within a reasonable period. **We recommend a provision to similar effect.**

Appropriateness of oath requirement

17.41 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 agency 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 not be empowered to obtain evidence on oath, but that instead it be a criminal offence to wilfully make a false statement.**

C. REVIEW AND APPEAL PROCEDURES

17.42 In keeping with our concern with 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. We favour the right to appeal on the merits of decisions made by a public authority vested with the quite extensive powers we have recommended for the Privacy Commissioner. But 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). 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 a specially constituted tribunal. The Tribunal would consist of three part-time members and be chaired by a legally qualified person. The Chairman would be assisted by a member experienced in information management and the third member would be a layman. Members would be appointed for three years, with the option of one reappointment. The hearing before the tribunal would not be a full rehearing, but would be restricted to a review of the correctness of the decision appealed from in the light of the evidence below, together with any new evidence or explanations provided by either party at the appeal hearing. A greater degree of formality is appropriate at this appellate level and parties would have the legal right to appear in person and, at the discretion of the Tribunal, through counsel. Evidence would be on oath. The Tribunal would have the power to award costs. It would give written reasons for its decisions. There would be a right of appeal from the Tribunal to a court on questions of law only.**

CHAPTER 18

TRANSBORDER DATA FLOW

SUMMARY

This chapter examines the controls which should be imposed on the transfer of data to countries 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 data which is controlled in Hong Kong, regardless of whether or not the data is held within the territory.

If the general provisions of the law accordingly apply to data which has been transferred to another country but is controlled here, no additional provisions are required dealing specifically with export. Should the export of data be accompanied by a loss of control of its use, however, we believe that specific measures may be required.

The majority of transfers of data overseas are either for public purposes or for purposes which involve the consent of the data subject. We do not think such transfers should be subject to additional controls, whether or not they also involve transfer of control. To avoid additional bureaucracy, these transfers should not require prior approval of the data protection authority. 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 country. This duty can be discharged in various ways, including the application of a data protection law in the other jurisdiction, sectoral codes of conduct, or contracts. Failure to adequately discharge the duty will expose the data exporter to intervention by the Hong Kong data protection authority.

RECOMMENDATIONS

(i) The general provisions of the data protection law should apply to the processing of personal data whether or not in Hong Kong, provided the data controller is in the territory. (paragraph 18.10)

Control of data is indicated by its collection, including the "capture" of data by, for example, an operator keying in instructions to another data user, whether or not the latter is in Hong Kong. (paragraph 18.11) Data processing within Hong Kong which is controlled from outside the territory should not be subject to the general application of the law, although certain provisions such as those relating to data security may be applied. (paragraph 18.10)

(ii) 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 18.13)

(iii) A data transfer to a third country which does not ensure an adequate level of protection may take place on condition that:

> 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 country which does not ensure an adequate level of protection;
>
> the transfer is necessary on important public interest grounds of the kind discussed in Chapter 15; or
>
> the transfer is necessary in order to protect the vital interests of the data subject. (paragraph 18.15)

(iv) As regards other cases, a specific legal obligation should be imposed on Hong Kong data users exporting data without retaining full control over its use in the other country. 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 exported 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 18.19)

(v) 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 importing country and the nature of the data. (paragraph 18.18)

DELIBERATIONS

A. Background

18.1 International data traffic necessarily entails transfers between countries with disparate legal systems. In her recent comprehensive review of the issue, 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 flow of transborder data ("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 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 countries. 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 to the formulation of these principles was to rationalise the international regulation of data flows through the harmonisation of national laws. By joining a number of other countries that have adapted or enacted laws to secure harmony with these principles (including within the region Japan and Australia), Hong Kong will be well placed to benefit from continued data traffic from its trading partners.

The need for transborder controls

18.2 Even countries possessing data protection laws often lack provisions controlling the export of data. Increasingly, however, the climate of international concern over "data havens" (countries without adequate privacy protection regulating data processing) is finding legal expression in domestic legislation. The whole issue has been highlighted by the European Communities Commission 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."*

18.3 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.

---

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

2 Nugter (1990), see note 1 above.

18.4 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.**

B. Territorial scope of data protection laws

18.5 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. It 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 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.

18.6 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.

18.7 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, insofar as the law applies where such control is exercised notwithstanding that the processing is carried out elsewhere. As regards computer bureaus, however, the determining factor is whether the processing is carried out in the UK.

---

[3] Wesley-Smith, Peter, *Consitutional and Administrative Law in Hong Kong*, (Hong Kong: China & Hong Kong Law Studies Ltd, 1988) pp.273-5.5.

18.8 A further variant is provided by the Netherlands law, whose territorial scope is primarily determined by whether the file is located within the country.

18.9 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.

18.10 In choosing an appropriate criterion to determine the territorial scope of a data protection law for Hong Kong, we consider the crucial factor to be whether the data use is controlled within Hong Kong, whether or not the processing is undertaken here. We also gave careful consideration to whether we also wished to fully regulate data processing within Hong Kong where the data controller is outside Hong Kong. We concluded that to do so generally could lead to practical problems. For example, it could be argued that Hong Kong Telecom processes all international telephone calls transmitted through Hong Kong, even though the calls originated and terminated outside the territory. We do not think that to the extent that Hong Kong data users act purely, as processing conduits between other countries, they should be subject to the full force of Hong Kong's data protection regime as regards such data. The application of some of the data protection principles will remain appropriate, however, such as that relating to data security. **We therefore recommend that the general provisions of the data protection law apply to the processing of personal data whether or not in Hong Kong, provided the data controller is in the territory. Data process within Hong Kong which is controlled from outside the territory should not be subject to the general application of the law, although certain provisions such as those relating to data security may be applied.**

18.11 Whilst we consider the control test generally adequate in determining the application of the law to data processors in Hong Kong, to avoid uncertainty we think it should be supplemented in one respect. **We recommend that data processing involved in the collection of data within Hong Kong should be subject to the application of the law. "Collection" in this context should extend to what may he characterised as the "capture" of data by, for example, an operator keying in instructions to another data user outside Hong Kong.** Such collections/captures could perhaps be viewed as evincing the exercise of control over data within Hong Kong. To this extent it may be viewed as a particular application of the control test rather than as a supplement to it.

C. Regulation of data exports not subject to general provisions of the data protection law

18.12 In view of this emphasis on the control of data, it does not follow from the export of data that it will cease to be subject to the full application of

the Hong Kong law. If data are exported but exclusive control is retained within Hong Kong (eg export to a data bureau solely for processing and return to Hong Kong for use), it 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 export is accompanied by a loss of control over the data. Accordingly all data exports 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 export of data not subject to the general application of the law should nonetheless be regulated.

Definition of transfer

18.13 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 its 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 export of data. A similar consistency is apparent in the UK law, although to the contrary effect as the law is restricted to the automatic processing of data. **We accordingly recommend the regulation of the export 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.**

The draft Directive and permissible data exports

18.14 One of the most significant alterations to the latest (15-10-1992) 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."

18.15 **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 control is retained within Hong Kong).

Transborder data regulation in other countries

18.16 In view of the above, we can restrict our attention to legal regulation of data exports which are neither subject to the general provisions of the data protection law (because the data are controlled from Hong Kong), nor falls 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]

4 (1988) *New Zealand Law Journal* P.384.

Approval requirements

18.17 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 alacrity 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 export. And 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 he 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 exports

18.18 We agree that the Privacy Commissioner should be able to intervene in circumstances such as these. We also agree that declarations play a pivotal role through the requirement that data users identify all countries to whom they propose exporting data, and specifying whether control will be retained within Hong Kong over that data. It is important that this be up-to-date and as with other alterations to material particulars of the declaration, data users should be required to lodge an amendment if the list of proposed transferee countries changes. But as a mechanism of intervention 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 importing country 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.**

A legal duty on data exporters

18.19 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 transfer not falling within the scope of article 26(2), we recommend imposing a specific legal obligation on Hong Kong data users exporting data without retaining full control over its use in the other country. 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 exported 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. Consistently with the role we envisage for him, the Privacy Commissioner would also be able to investigate possible breaches at his own initiative.**

Methods of satisfying duty to ensure compliance following export

18.20 At first blush it may appear unduly onerous to require data users to take steps to ensure that a transferee in another country comply with the data protection principles where control over its use was 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 countries. 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 country 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 countries 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.

Voluntary codes of conduct

18.21 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.

Contractual assurances of compliance

18.22 The other main method of securing compliance by a transferee in a country 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 exporter). 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 the Privacy Commissioner have in relation to the Hong Kong based transferor.

18.23 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 exports on a case by case by basis, other than by having proposed transferee countries identified in declarations. In the first instance it would be a matter for the Hong Kong data exporter 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 exporter 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 exporter had discharged the legal duty we propose to apply.