

THE LAW REFORM COMMISSION OF HONG KONG

REFORM OF

THE LAW RELATING TO THE PROTECTION OF PERSONAL DATA

SUMMARY

(This is a summary of the Law Reform Commission's Report on "Reform of the Law Relating to the Protection of Personal Data". While it contains the full text of the recommendations contained in the Report and summarises the supporting discussion, those wishing more detailed explanation should refer to the report itself. References to the relevant passages in the report are listed overleaf).

**SUMMARY OF THE THE LAW REFORM COMMISSION
OF HONG KONG REPORT ON REFORM OF
THE LAW RELATING TO
THE PROTECTION OF PERSONAL DATA**

	<u>Page</u>	<u>Reference to Report</u>
INTRODUCTION	1	Introduction p.1 – p.7
1 THE INFORMATION BOOM	4	Chapter 1 p.8 – p.13
2 INFORMATION PRIVACY IN THE INTERNATIONAL CONTEXT	4	Chapter 2 p.14 – p.27
3 THE PROTECTION OF PERSONAL DATA IN HONG KONG: THE NEED FOR REFORM	7	Chapter 3, 4 & 5 p.28 – p.72
4 OBJECTIVES AND SCOPE OF A DATA PROTECTION LAW	9	Chapter 6, 7 & 8 p.73 – p.95
5 COLLECTION OF PERSONAL DATA	10	Chapter 9 p.96 – p.112
6 REGULATION OF THE USE AND DISCLOSURE OF PERSONAL DATA	12	Chapter 10 p.113 – p.128
7 PINS AND DATA MATCHING	13	Chapter 11 p.129 – p.146
8 DATA QUALITY AND SECURITY	15	Chapter 12 p.147 – p.156
9 OPENNESS AND DATA PROTECTION	16	Chapter 13 p.157 – p.167
10 DATA SUBJECTS' RIGHTS OF ACCESS AND CORRECTION	18	Chapter 14 p.168 – p.179
11 EXEMPTIONS	20	Chapter 15 p.180 – p.208
12 STRUCTURE, FUNCTIONS AND POWERS OF THE PRIVACY COMMISSIONER	23	Chapter 16 p.209 – p.233

13 TRANSBORDER DATA FLOW

**28 Chapter 17
p.234 – p.243**

14 THE MEDIA AND DATA PROTECTION

**29 Chapter 18
p.244 – p.262**

INTRODUCTION

Terms of reference

1. On 11 October 1989 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 communications of the information or opinions referred to in paragraph (a) to any person or body including any Government department, public body, person or corporation in or out of Hong Kong;*
- (c) intrusion (by electronic or other means) into private premises; and*
- (d) the interception of communications, whether oral or recorded;*

but excluding inquiries on matters falling within the Terms of Reference of the Law Reform Commission on either Arrest or Breach of Confidence."

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

What is privacy?

3. A key word in the terms of reference is "privacy". Despite the huge literature on the subject, there is no satisfactory definition of the term "privacy". Studies in this area have generally concluded that the most satisfactory way of defining what is meant by privacy is by reference to the interests that privacy seeks to protect. We have therefore tried to identify and define the interests which are invariably raised in any discussion of "privacy", to explore the extent of their legal protection, and to determine whether additional protection is warranted.

4. Those "interests" are:

- (a) the interest of the person in controlling the information held by others about him, or "information privacy";
- (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".

5. Item (a) ("information privacy") corresponds to paragraphs (a) and (b) of our terms of reference. It is this aspect of "privacy" that is dealt with in this report.

6. The terms of reference refer to information and opinions relating to individuals. The nature of information about individuals varies enormously, from publicly available data, such as names and addresses of telephone subscribers, to intimate data referring to an individual's sexual activities. For the purposes of this report, "personal information" refers to any information relating to an identifiable individual, regardless of how apparently trivial it may be. Information about intimate aspects of an individual's private life will be referred to as "sensitive information".

7. Other points worth nothing about the terms of reference are:

- (a) Whilst "information" is a readily understood term, this report will refer to "data" rather than "information". In particular, the expression "data protection" is frequently used. The literature tends to use "information" and "data" interchangeably, but there is a difference between them. Broadly speaking, any record (however fleeting) or representation amounts to data; information is the interpretation that an observer applies to these records or representations. "Data" can therefore be said to be "potential information". Because this report's concern is largely with information records, and also to accord with international usage, "data" will be used unless "information" is more apt. It should be stressed that this report is concerned only with *personal* data. All reference to "data" are "personal data".
- (b) "Remedies" includes, 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, or administrative or 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

8. The Law Reform Commission appointed a sub-committee to examine the current state of legal protection and to make recommendations. Its membership was as follows:

The Honourable Mr Justice Mortimer, Member of the Court of Appeal, Chairman

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

Mr Don Brech, former Director, Government Records Service

Mrs Patricia Chu, Assistant Director, Social Welfare Department

Mr Con Conway, Director of Community Affairs, Hong Kong Telecom

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

Mr James O'Neil, Deputy Principal Crown Counsel, Attorney General's Chambers

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

Mr Peter So, Deputy Commissioner of Police (Management), Royal Hong Kong Police Force

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

Mr Wong Kwok Wah, Managing Editor, Sunday Chronicle

Mr Mark Berthold, Consultant, Law Reform Commission (Secretary)

9. Over the period of three years preceding the release of its Consultative Document, the sub-committee reviewed the relevant legal and specialist literature in 56 meetings. Input was obtained from officials and

experts from other jurisdictions. The sub-committee publicly released its interim proposals in its Consultative Document on 17 March 1993 and sought submissions from interested parties. The consultative period concluded on 1 August and featured numerous seminars arranged by professional organisations. Over 80 detailed submissions were received and these were carefully considered by the sub-committee over the course of 20 additional meetings. With only three exceptions the submissions received evince broad support for a law regulating personal data in both the public and private sectors. Public attitudes were also gauged by means of a public attitudes survey conducted by Dr. John Bacon-Shone and Dr. Harold Traver. The survey results indicated public support for the principles of data protection.

10. The sub-committee's final report was considered by the Law Reform Commission at six meetings held between 24 May 1994 and 12 July 1994.

1. THE INFORMATION BOOM

1.1 Much of the impetus to increased legal protection for privacy derives from the "information boom". 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. Nonetheless non-automated paper files continue to be the repository of much personal data.

1.2 Computers have undergone a revolution of their own by evolving from large mainframes to microcomputers which are far more powerful than their larger predecessors. Properly used, computers 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.

2. INFORMATION PRIVACY IN THE INTERNATIONAL CONTEXT

2.1 Two international aspects of information privacy relevant to any discussion of legal reforms in Hong Kong are:

- (i) internationally recognised data protection principles and the development and implications of transborder data flow regulation; and
- (ii) human rights law.

These two aspects will now be briefly examined.

The data protection principles

2.2 All data protection legislation is founded on a set of data protection principles. The three most influential sets of principles are those contained in :

- (i) the Council of Europe's 1980 *Convention for the Protection of individuals with regard to Automatic Processing of Personal Data*. This is the basis for various European data protection laws;
- (ii) the Organisation for Economic Co-operation and Development's 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* ("the OECD Guidelines", which are the basis for the laws of a number of Member States, including Australia, New Zealand and Japan. They are also the main basis of voluntary Guidelines adopted in Hong Kong in 1988. They cover essentially the same matters as those of the Council of Europe, except that they include non-automated data; and
- (iii) the Commission of the European Communities' 1992 *Amended proposal for a Council Directive on the Protection of Individuals With Regard to the Processing of Personal Data* ("the draft Directive"). This 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.

2.3 In formulating our recommendations, we have adopted the OECD Guidelines. The OECD Guidelines define "personal data" as "any information relating to an identified or identifiable individual (data subject)". The OECD Guidelines identify the following principles:

1. "Collection Limitation Principle"

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

2. "Data Quality Principle"

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

3. "Purpose Specification Principle"

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

4. "Use Limitation Principle"

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

- (a) with the consent of the data subject; or
- (b) by the authority of law.

5. "Security Safeguards Principle"

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

6. "Openness Principle"

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

7. "Individual Participation Principle"

An individual should have the right:

- (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- (b) to have communicated to him, data relating to him
 - (i) within a reasonable time;
 - (ii) at a charge, if any, that is not excessive;
 - (iii) in a reasonable manner; and
 - (iv) in a form that is readily intelligible to him;

- (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
- (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

8. "Accountability Principle"

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

3. THE PROTECTION OF PERSONAL DATA IN HONG KONG - THE NEED FOR REFORM

Summary

3.1 Pressing international trade considerations argue for early recognition of the standards of privacy protection contained in the internationally agreed data protection principles. Twenty-seven jurisdictions have data protection laws based upon either the Council of Europe Convention or the OECD Guidelines. The developing trend is that countries lacking laws incorporating the data protection principles will be denied general access to personal data held by countries with such laws. This is specifically envisaged by the European Communities Commission draft Directive scheduled for implementation in 1996.

3.2 We examine the extent to which the international standards are recognised in the existing statutory and common law in Hong Kong. Existing statutory protection of information privacy is scattered and incidental in nature. Article 14 of the Bill of Rights Ordinance is the sole legislative provision specifically providing for privacy of information. 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. Its focus on information relating to a person's private life is narrower than the OECD Guidelines' concern with any information relating an individual. Also, its application is limited to the public sector and does not address private sector infringements.

3.3 A number of ordinances include provisions relating to personal records held for diverse purposes such as education, employment, taxation, immigration, census and statistics, insurance, registration of persons and venereal disease. The ordinance are not uniform in approach but patterns can be discerned. Some require the data subject to provide information directly, whereas others which require the compilation of records do not expressly so stipulate.

3.4 Other authorities are specially empowered to obtain information from record keepers, but this power is usually (not invariably) limited by a

secrecy provision imposed upon the recipient. Further, in general these ordinances do not expressly sanction the transfer of personal information between governmental agencies. Hong Kong has no archives or records legislation providing a statutory basis for the management of records by government agencies.

3.5 In addition to the limited protection of information privacy provided by local legislation, the common law provides some protection. The two common law doctrines of greatest relevance are:

- (i) the duty 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 those of doctor/patient and banker/customer. The limited remedy provided by breach of confidence is nonetheless the only common law doctrine specifically directed at restricting the disclosure of personal information; and
- (ii) the legal protection against unauthorised disclosure provided by the law of contract, either by express or implied terms in the contract.

3.6 Other, less relevant, legal principles are public interest immunity, legal professional privilege, copyright, defamation and negligence.

3.7 We also 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

3.8 We recommend that the internationally agreed data protection principles should be given statutory force in both the public and private sectors. We further recommend the adoption of the OECD Guidelines as the appropriate formulation of the data protection principles. Insofar as that formulation differs in substance from the Hong Kong voluntary guidelines, we recommend that preference be given to that of the OECD formulation. In addition to the OECD Guidelines, we have also paid close attention to the more comprehensive framework provided by the European Communities Commission's revised draft Directive. Many of our recommendations detailed below reflect this.

3.9 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.

4. OBJECTIVES AND SCOPE OF A DATA PROTECTION LAW

Summary

4.1 We considered the scope of a law giving effect to the data protection principles and conclude that such a law should be concerned with "personal data" in the broad sense of any representation of information relating to an identifiable individual. This corresponds to the OECD Guidelines.

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

Recommendations

4.3 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 they relate. The data to be regulated must, however, be disposed in such a way as to enable access to required data to be practicably obtained whether by automated means or otherwise. However, all data (regardless of its level of retrievability) must be protected by reasonable security safeguards.

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

- (i) the data quality principle applies. There should be no right to compensation for a breach of this principle during this period.
- (ii) the data subject access provisions fully apply. The data user would not be obliged to provide a full copy of all data held at the time of the request, but would be entitled first to clean up the data by updating and removing irrelevant or dubious data. He would then be obliged to provide the data subject with a copy of all the remaining data. Upon expiration of the transition period

he would lose the right to alter data before responding but would be required to provide a copy of all the data held upon receiving the request.

5. COLLECTION OF PERSONAL DATA

Summary

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

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

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

Recommendations

5.4 We recommend that the broad principles contained in our scheme should be supplemented by more detailed sectoral codes of practice. These codes of practice should not be given legal force, nor the power to qualify the provisions of the data protection law, but compliance with a

sectoral code approved by the Privacy Commissioner should be taken into account in determining whether there has been a breach of the principles.

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

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

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

- (a) the data are collected, acquired or held for a lawful purpose directly related to a function or activity of the collector; and
- (b) the collection, acquisition or storage is necessary for, or directly related to, that purpose.

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

- (a) the purposes of the processing for which the data are intended;
- (b) the obligatory or voluntary nature of any reply to the questions to which answers are sought;
- (c) the consequences for him if he fails to reply;
- (d) the recipients or categories of recipients of the data;
- (e) the existence of a right of access to and rectification of the data relating to him; and
- (f) the name and address of the controller and of his representative if any.

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

5.8 A data subject from whom data are collected without his knowledge through automatic metering should be informed of the frequency of data collection, the time of their storage, and the use to be made of the data. If this is not feasible the collection of data should be subordinated to legal authorization.

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

- (a) the data subject's consent should be required prior to the installation of any relevant equipment in his real or personal property under his control.
- (b) only personal information which is necessary for service or billing purposes should be collected and stored.

6. REGULATION OF THE USE AND DISCLOSURE OF PERSONAL DATA

Summary

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

- (i) data purposes must be specified in writing and communicated to a third party, usually the data protection authority (“the Privacy Commissioner”). 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

6.2 The purposes for which data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes.

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

- (a) with the consent of the data subject; or
- (b) by the authority of law, including one of the use limitation exemptions discussed in Section 11 below.

6.4 Users of personal data should specify all data purposes in a declaration to be furnished to the Privacy Commissioner. This would be purely a notification procedure and the Privacy Commissioner would not be required to approve the data uses.

6.5 The Business registration scheme should be made the principal means of identifying private sector holders of personal data and bringing them within the scope of regulation. The current business registration forms should be modified for this purpose. 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 data purposes and contact details of the responsible officer

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

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

6.8 Data subjects should not be deemed to have knowledge of specified data uses contained in public declarations.

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

6.10 Each functionally distinct government department or branch and each company should constitute a separate data user.

7. PINS AND DATA MATCHING

Summary

7.1 There are two related concerns:

- (i) the information privacy implications of personal identity numbers ("PIN's"); and
- (ii) the matching across databases of data relating to an individual.

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

7.3 The main privacy peril arising from PIN's is their role in facilitating data matching. PIN's are keys to matching across databases. 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. This is particularly so with investigative matching programs aimed at identifying discrepancies and taking administrative action against data subjects.

Recommendations

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

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

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

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

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

being identified as a "hit". Also relevant is whether it is proposed to inform data subjects in advance.

- (b) The guidelines should also set out procedures according "hits" the right to correct matching results before adverse decisions are taken on their basis.
- (c) The onus should be on organisations to show a competing social need which overrides the privacy interests of data subjects. The justification for the data matching programme should include an outline of why alternative means of satisfying the objectives are less satisfactory, and a cost/benefit analysis of the program.

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

8. DATA QUALITY AND SECURITY

Summary

8.1 The OECD Data Quality Principle requires that in the interests of both the data subject and data user, 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.

8.2 Incorrect data can arise through inadvertent computer error, technical failure, or intentional misuse. Intentional misuse, and in particular unauthorised access (popularly known as "hacking"), has received considerable public attention.

8.3 We also make recommendations implementing the OECD Security Safeguards Principle. This 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

8.4 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 the data are identified as such,

or where the inaccuracy occurs despite all reasonably practicable steps being taken.

8.5 Data which are inaccurate or incomplete having regard to the purpose for which they are held, should be erased or rectified. Data should not be kept in a form which permits identification of the data subject any longer than necessary for the fulfilment of the data purposes.

8.6 Data users should be subject to the duty to take such reasonably practicable steps as are necessary to correct data transferred, having regard to the nature and effect of the data.

8.7 Data users should be required to take all reasonably appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of, both automated and manually stored personal data and against accidental loss or destruction of such data.

In determining the scope of this duty, regard shall be had to -

- (a) the nature of the personal data and the harm that would result from such access, alteration, disclosure, loss or destruction as are mentioned in this principle; and
- (b) the place where the personal data are stored, to security measures programmed into the relevant equipment and to measures taken for ensuring the reliability of staff having access to the data.

9. OPENNESS AND DATA PROTECTION

Summary

9.1 The OECD Openness Principle has both general and specific aspects. The former requires that the public be advised of the nature and scope of record systems to promote the scrutiny of administrative and technological developments affecting data protection. The latter stipulates that means must be available for an individual to ascertain whether data is held concerning him. We have concluded above that this could be achieved by a requirement that the data user furnish the data protection authority with a declaration describing his data purposes.

9.2 We now develop that proposal. Our aim is to restrict the contents of declarations to the bare essentials. The vast majority of personal data users are small businesses engaged in a limited number of common data purposes. To facilitate completion, we think that the declaration for mainstream data purposes should be in a multiple-choice format. As public sector declarations should be more comprehensive, they will not be susceptible to a multi-choice format.

9.3 We consider easy access to the contents of declarations by interested individuals is essential if data subjects are to be able to effectively exercise their rights of data access and correction.

Recommendations

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

- (a) by the Privacy Commissioner in the carrying out of his functions
- (b) by the Administrative Appeals Board and the courts
- (c) in the formulation and approval of sectoral codes.

9.5 Public sector users of personal data should compile declarations describing the following features of a personal records system:

- (a) the purposes for which the data are kept;
- (b) the content of data contained in the classes of record, including any sensitive content, namely data revealing racial or ethnic origin, political opinions, religious beliefs, philosophical or ethical persuasion or trade union membership, and of data concerning health or sexual life;
- (c) the classes of individuals about whom records are kept;
- (d) to whom the data are usually disclosed;
- (e) the functional title and contact details of the individual (the responsible officer) who can provide information to data subjects about access to their personal data; and
- (f) jurisdictions to which personal data are exported

9.6 Private sector data users should compile declarations identifying all data purposes and contact details of the responsible officer. The Privacy Commissioner should be empowered to prescribe the forms to be used in making declarations.

9.7 Although a data user is only required to lodge one declaration, separate entries should be made for each data purpose.

9.8 For mainstream small business users the declaration should take the form of a structured multi-choice questionnaire. This will accommodate a small number of data purposes which are commonly engaged in.

9.9 The establishment of a system providing interested individuals with on-line access to the contents of declarations of organisations.

9.10 Every data user should designate a responsible officer to facilitate compliance. The officer may be jointly liable with the organisation for a breach of the data protection principles.

10. DATA SUBJECTS' RIGHTS OF ACCESS AND CORRECTION

Summary

10.1 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.

10.2 This principle gives data subjects access and correction rights. These rights are fundamental to the operation of an effective scheme to regulate the use of personal data and are described in the OECD Explanatory Memorandum as "perhaps the most important privacy protection". We conclude that it is not feasible for a data protection authority to have the exclusive role of monitoring compliance and it is essential to involve data subjects in the process if it is to be effective.

Recommendations

10.3 Access and correction rights should not be restricted to Hong Kong residents.

10.4 An interested individual should be legally entitled to be informed by a data user whether the latter's data refer to that individual; and if so, to be supplied with a copy of that data.

10.5 Upon receipt of an inquiry as to whether data exist which is unaccompanied by a request for such data, the data user should have a discretion as to whether he shall provide a copy of that data at that stage, or to await a specific request for a copy.

10.6 A nominal, waivable, fee should be payable by a data subject for inquiring as to whether data exist relating to him. A nominal (not cost-related) fee should be payable for full access requests which require the supply of a copy of data held, to deter mischievous requests. It should operate as a maximum, and organisations should be at liberty to reduce or even waive it. A fee may be charged on a commercial basis if a copy had been provided earlier.

10.7 Access fees should be provided for in subsidiary legislation and in a manner facilitating their updating as required.

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

10.9 Data provided in response to access requests should be in an intelligible form, unless they are contained in a true copy of a written document which is unintelligible on its face. Data should be supplied in the language in which it is held and where data is held in more than one language, it should be provided in both languages.

10.10 Access requests be complied with within 45 days.

10.11 A data user should not be required to respond to subject access requests:

- (a) unless he is supplied with such information as he may reasonably require in order to satisfy himself as to the identity of the person making the request and to locate the information which he seeks; or
- (b) to the extent that he cannot comply with the request without disclosing information relating to another individual who can be identified from that information, unless he is satisfied that the other individual has consented to the disclosure of the information to the person making the request. The reference to information relating to another individual is restricted to a reference to information naming or otherwise explicitly identifying that individual as the source of information.

10.12 Whenever the data user withholds data on the basis of a statutory exemption, the data user should be legally required to inform the data subject of the exemption claimed unless doing so is likely to prejudice the purposes for which the data are kept or cause other serious harm. In such cases, data users should keep a log of cases in which a subject exemption is relied upon and the reasons for the exemption's use. The log should be available for inspection by the data protection authority and the authority should also be provided with a periodic return.

11. EXEMPTIONS

Summary

11.1 Data protection laws seldom attempt to regulate all data uses. Two alternative approaches are possible:

- (i) a law of general application but with specific exemptions; or

- (ii) a law restricted to specified data users.

11.2 We propose adopting the first of these alternatives. This is the approach generally adopted in other jurisdictions and makes it easier to amend the law as circumstances change.

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.

11.3 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.

11.4 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."

11.5 Our recommendations on this are concerned with the exemptions to be included in the principal data protection legislation. Other ordinances will also effect partial exemptions.

Recommendations

11.6 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.

11.7 No exemption from the application of the data protection law should be made for non-profit making bodies.

11.8 The Use Limitation Principle should not apply:

- (i) to data required by or under any enactment to be made available to the public;

- (ii) where it would be likely to prejudice the prevention of serious injury or other damage to the health of any person, the prevention or detection of crime, the apprehension, prosecution or detention of offenders, or the assessment or collection of any tax or duty;
- (iii) where the disclosure relates to conduct that is illegal or seriously improper and the person making the disclosure had reasonable grounds for believing that the disclosure to the person receiving it would contribute to the prevention or remedying of the unlawful or seriously improper conduct ; or
- (iv) where the disclosure relates to the character or activities of an individual where this is likely to seriously affect the performance of the functions of a statutory body or administrative tribunal.

11.9 The Privacy Commissioner may exempt research data that has not been irreversibly anonymised from the application of the Purpose Specification and Use Limitation Principles. In providing his consent the Privacy Commissioner would need to be satisfied that the research is in the public interest, having regard to the following safeguards:

- (i) whether access to data identifying individuals is necessary for the scientific validity of the research;
- (ii) whether access to that data without the data subject's consent is justifiable in the circumstances;
- (iii) whether the research has undertaken to comply with the relevant code of conduct; and
- (iv) whether the research results are to be anonymised, except to the extent that this is outweighed by the public interest.

11.10 There should be an exemption from access and correction rights:

- (i) to the extent that the release of the data would be likely to prejudice the prevention or detection of crime, the apprehension, prosecution or detention of offenders, the assessment or collection of any tax or duty, regulation of financial institutions, markets and industry, or identify any individual disclosing data within the scope of the exemption from the Use Limitation Principle specified in paras. (iii) and (iv) of paragraph 11.8.
- (ii) to data received from third parties relevant to the making of judicial appointments;
- (iii) to data to which a claim for legal professional privilege can be made out;

- (iv) to data the release of which is likely to cause serious harm to the physical or mental health of the data subject;
- (v) to staff succession planning data;
- (vi) interim access to data relating to an evaluative process which will be seriously disrupted by affording access before a decision has been made and where appeal rights exist. The data must be retained following the making of the decision, when access rights accrue; and
- (vii) personal references supplied on a confidential basis by a person not under a duty to supply these to the organisation seeking to fill a vacancy. The exemption should cease to apply upon the position being filled.

11.11 For the avoidance of doubt, the statutory definition of "personal data" to which the access provisions apply should expressly exclude criteria of general application. Insofar as a decision may be expressed cryptically, the requirement that the data be provided in an intelligible form does not entail the decoding of the applicable criteria.

11.12 Except in the case of data held for the purposes of the security, defence or international relations in respect of Hong Kong, the Privacy Commissioner shall upon application review the release of data where the data user has claimed an access exemption. The initial responsibility in fully responding to access requests lies with the data user. The statutory language should make it clear that access requests should be complied with insofar as it is possible to do so without prejudicing the exempted purpose.

11.13 Data held for the purpose of the security, defence or international relations in respect of Hong Kong should be exempted from access and correction rights and from the application of the Use Limitation Principle whenever that interest is likely to be otherwise prejudiced. A certificate personally signed by the Governor or Chief Secretary would be evidence of the exemption. This power should not be delegable. Data users would nonetheless remain subject to the general requirement of furnishing declarations describing in general terms the data held for these purposes. In addition, the other data protection principles would apply. As regards the data identified in the certificate, he would be entitled to look behind the certificate of the Governor or Chief Secretary to confirm that the data purpose for which the exemption was claimed was correctly classified as relating to the security, defence or international relations in respect of Hong Kong.

11.14 Upon receiving a complaint concerning data relating to the security, defence or international relations in respect of Hong Kong, the Privacy Commissioner should be entitled to monitor compliance with the data protection principles. The Privacy Commissioner will only indicate to the data subject that he has made all necessary inquiries and will not disclose whether

there is a file on the inquirer. This will preclude the complainant from pursuing any appeal to the tribunal.

11.15 The Council of Europe recommendations regulating the use of personal data in the police sector should be used as the basis for deriving a similar code suitable for Hong Kong.

12. STRUCTURE, FUNCTIONS AND POWERS OF THE PRIVACY COMMISSIONER

Summary

12.1 If the detailed regulatory framework governing the use of personal data we have recommended about 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. We propose the establishment of such an authority, which we refer to as "the Privacy Commissioner".

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

12.3 Our recommendations on this address the structure, functions and powers appropriate for the Privacy Commissioner. We think the Privacy Commissioner should have an investigative role and be assisted in policy formulation by a board.

12.4 We consider the independence of the Commissioner is fundamental. This requires adequate safeguards in the making of appointments, security of tenure for those appointed, and a budget sufficient to fulfil the authority's functions effectively.

12.5 We believe that the Commissioner should not be restricted to responding to complaints but should be able to initiate his own investigations and on-site inspections.

12.6 Data users will have to provide the declarations described in previous sections to the Commissioner. The Commissioner will approve sectoral codes of practice and publicise data protection requirements.

12.7 We believe that powers to enter premises and obtain evidence are necessary to enable the Commissioner to carry out his functions. The data user's consent should first be sought but, if that is not forthcoming, the court should be empowered to make an appropriate order for entry and seizure.

12.8 We consider that disputes between data subjects and data users should be referred to the Administrative Appeals Board.

Recommendations

12.9 Overseeing observance with the regulatory requirements of a data protection law should be the sole responsibility of an independent authority established for the purpose. In addition to assisting individuals to enforce their rights, the authority should perform a number of other functions, including the investigation of complaints, the provision of a central notification point for data users furnishing declarations describing their personal data systems, the conduct of on-site verifications regarding the operation of such systems, and the carrying out of educational and publicity functions. The authority is referred to as the "Privacy Commissioner".

12.10 The full-time Privacy Commissioner should be assisted in the formulation of policy by a board of five part-time members of high standing representing the public and private sectors with not more than one government servant and at least one member having extensive experience in data processing. There should be no maximum age limit. The board of commissioners should meet not less than quarterly.

12.11 The Privacy Commissioner and the commissioners should be appointed by the Governor. The Privacy Commissioner should be appointed for a term of five years with the option of not more than one further appointment. Part-time commissioners should be appointed for a term of three years, with the option of not more than two further appointments.

12.12 The tenure of the Privacy Commissioner should be protected by a provision requiring that he may only be removed from office by the Governor with the approval by resolution of the Legislative Council on the ground of inability to discharge the functions of office, or misbehaviour. Members of the board of commissioners may be dismissed by the Governor alone.

12.13 To secure an adequate budget, an annual levy of \$100 should be levied on all applicants for business registration.

12.14 The Privacy Commissioner should have the following functions:

- (a) investigation of complaints;
- (b) the conduct of on-site inspections of data users;
- (c) notification point for declarations from data users;
- (d) promoting codes of practice; and
- (e) educational and publicity functions.

12.15 The Privacy Commissioner should investigate any complaint that any of the data protection principles or provisions of the data protection law

have been, or are being, contravened. He should be expressly empowered to initiate investigations in the absence of a complaint, provided he has reasonable grounds for suspecting a breach of the data protection law.

12.16 The Privacy Commissioner should have a limited discretion to decline to investigate complaints on well-established grounds regarding lack of merit.

12.17 Data subjects should have the right to complain direct to the Privacy Commissioner. 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.

12.18 There should be provision for class complaints along the lines that, in the case of an act or practice that may be an interference with the privacy of two or more individuals, any one of those individuals may make a complaint.

12.19 The Privacy Commissioner should have the discretion to regulate his own procedures, subject to safeguards regarding fairness. The respondent should be informed at the outset that a complaint against him has been received. The Privacy Commissioner should be able to hear or obtain information from such persons, and make such inquiries, as he thinks fit. A person should only be entitled to be heard by the Commissioner if the Commissioner is proposing to make an adverse report or recommendation on him.

12.20 When a hearing is necessary, it should be held in public unless the data subject requests otherwise, in which case the hearing should be in private. 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.

12.21 The Privacy Commissioner should inform both parties in writing of the result of his investigation. Should he exercise his discretion and decline to conduct an investigation, or to take enforcement action following investigation, he should advise the complainant in writing of his decision or opinion and his reasons.

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

12.23 Upon finding a complaint substantiated, the Privacy Commissioner should be empowered to direct the remedy of the breach in a specified manner. The data user's Responsible Officer should be subject to a duty to notify the Commissioner that compliance has been effected. Failing compliance, the Commissioner should seek an enforcement order in court. If

compliance with the data protection principles cannot be adequately secured by an enforcement order, the Privacy Commissioner should apply to the court for an order prohibiting the organisation from processing personal data.

12.24 A right to compensation should accrue from any breach of the data protection principles causing loss or injured feelings. The Privacy Commissioner's role in compensation claims should be limited to determining whether there has been a breach of the principles. Upon his so certifying it should be for a court to determine the appropriate amount of compensation payable, if any. The status of the certificate in the court proceedings will be that of *prima facie* evidence, rebuttable on the balance of probabilities.

12.25 The Privacy Commissioner should have the power to initiate systematic on-site inspections of personal data systems. The purpose of the power would be to check that the data protection principles are being complied with and that appropriate control systems are in place. This should include verifying the accuracy of the organisation's declaration and extend to a physical examination of the operational adequacy of such aspects as storage security. It should be expressly provided that the power be exercised in a manner that does not unduly disrupt the organisation's daily operations. The board of commissioners should approve the schedule of data users selected for on-site inspections.

12.26 The Privacy Commissioner and his staff should be subject to a legal duty of secrecy subject to criminal sanctions.

12.27 The Privacy Commissioner should not be required to approve data uses described in declarations. The extent of his legal duty in responding to declarations should be to store them in a publicly accessible form. He should be empowered, however, to require further and better particulars when he sees fit.

12.28 Where a prosecution follows an offence under the data protection law, summary offences should face a maximum fine of \$50,000. Indictable offences should face an unlimited fine as well as the destruction or amendment of the offending data. The Privacy Commissioner should be required to compile an annual report to the Governor which should also be laid before the Legislative Council.

12.29 Where in the exercise of his functions the Privacy Commissioner requires entry to premises, the following procedures should be adopted:

- (a) where entry is not urgent, the Commissioner should initially approach the organisation's Responsible Officer. If consent is not forthcoming at that stage, the Commissioner should serve a notice advising that if consent is not received within 14 days then he will seek a court order and apply for costs.
- (b) where entry is urgent, the Commissioner should approach the court forthwith, thereby dispensing with the 14 day grace period.

In such cases, the Commissioner will consider it inadvisable to alert the organisation to his imminent visit (eg to avoid the destruction of evidence) and he should be empowered to approach the court direct for an order along the lines of an *Anton Piller* order authorising entry and seizure.

12.30 The Privacy Commissioner should be empowered to serve notice on any person requiring that person to furnish in writing such information or to produce any document or thing as is necessary or expedient for the performance of the Commissioner's functions. Such a notice should be appealable to a court. The necessary legal provisions should also address such ancillary matters as over-riding secrecy provisions, limiting the use of answers in other proceedings, and restrictions where it is certified that public interests such as security in respect of Hong Kong may be prejudiced.

12.31 The Privacy Commissioner should be empowered to seize any material, whether or not it may be subsequently ascertained that it is subject to an exemption, provided that he has reasonable cause to suspect that the data protection law has been contravened in respect of some of its contents and that any exempt data are returned within a reasonable period.

12.32 The Privacy Commissioner should not be empowered to obtain evidence on oath, but it should be a criminal offence to wilfully make a false statement to the Commissioner.

12.33 The Privacy Commissioner's decisions should be subject to judicial review. There should also be a right to appeal on the merits of decisions made by the Privacy Commissioner. Such appeals by data users and data subjects should be considered by the Administrative Appeals Board.

13. TRANSBORDER DATA FLOW

Summary

13.1 This section examines the controls which should be imposed on the transfer of personal data to jurisdictions lacking adequate data protection, whether or not the transfer is by automated means. It raises the question of the territorial scope of a data protection law in Hong Kong. We conclude that Hong Kong's data protection law should apply to any personal data which is processed or controlled in Hong Kong, regardless of whether or not the personal data is held within the territory.

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

13.3 We do not think that transfers of data outside the jurisdiction either for public purposes or for purposes which involve the consent of the data subject should be subject to additional controls, whether or not they also involve transfer of control. Those transferring data not falling within these categories should be subject to a duty to take all reasonably practicable steps to ensure that the data protection principles apply to the data while held in the other jurisdiction. This duty can be discharged in various ways, including the application of a data protection law in the other jurisdiction, sectoral codes of practice, or contracts. Failure adequately to discharge the duty will expose the data transferor to intervention by the Hong Kong data protection authority.

Recommendations

13.4 The general provisions of the data protection law should apply to the processing of personal data in Hong Kong, whether or not the data controller is in the territory. Equally, data processing outside Hong Kong which is controlled from within the territory should also be subject to the general application of the law.

13.5 The transfer of data out of Hong Kong should be legally regulated, regardless of the medium by which it is transferred. It should also extend to a telecommunications link not necessarily entailing its being recorded by the international recipient.

13.6 A data transfer to another jurisdiction which does not ensure an adequate level of protection may take place on condition that:

- (i) the data subject has consented to the proposed transfer in order to take steps preliminary to entering into a contract;
- (ii) the transfer is necessary for the performance of a contract between the data subject and the controller, on condition that the data subject has been informed of the fact that it is or might be proposed to transfer the data to a country which does not ensure an adequate level of protection;
- (iii) the transfer is necessary on important public interest grounds of the kind discussed in Section 11 above; or
- (iv) the transfer is necessary in order to protect the vital interests of the data subject.

13.7 As regards other cases, a specific legal obligation should be imposed on Hong Kong data users transferring data without retaining full control over their use in the other jurisdiction. The content of this duty would be that data users should take all reasonably practicable steps to ensure that the transferee complies with the data protection principles as regards the transferred data. The duty is distinct, however, from the duty of care contained in the legal action of negligence, as it would not be directly

enforceable by data subjects in the courts. Instead, as with the breach of the data protection principles, a breach would constitute the basis of a complaint to be investigated by the Privacy Commissioner. He would also be able to investigate possible breaches at his own initiative.

13.8 The Privacy Commissioner should be empowered to apply for an injunction when he has reasonable grounds for suspecting that a proposed transfer would result in a breach of the data protection principles. Relevant considerations would include the adequacy of data protection in the jurisdiction to which the data are transferred and the nature of the data.

14. THE MEDIA AND DATA PROTECTION

Summary

14.1 The main data protection issue we did not address in the Consultative Document was the scope of an exemption to accommodate free speech rights of the media. While we had recommended qualification on the application of the data protection principles to other competing public interests, this issue we deferred. This is a complex issue requiring analysis of the extent to which "free speech" rights exercised by "the media" should be constrained by the protections afforded by the data protection principles. The relevant parameters are provided by the Bill of Rights and our overall recommendations for an exemptions scheme. Also relevant is the extent to which alternative remedies are available to individuals adversely affected by the activities of the media. The extent to which free speech is already subject to both common law and statutory restrictions is an additional consideration.

Recommendations

14.2 Exemption applicable to the media should be restricted to data solely used for journalistic purposes.

14.3 The Collection Limitation Principle should apply to the media.

14.4 The Data Quality Principle should apply to the media. The media should be required to take all practicable steps to disseminate a correction where inaccurate data has been published.

14.5 There should be an exemption from the Use Limitation Principle for data the publication of which is in the public interest.

14.6 There should be a total exemption from the principle granting access and correction rights for unpublished data held by the media solely for journalistic purposes.

14.7 The Privacy Commissioner should be restricted to the reactive role of investigating complaints about the media. He should not be

empowered to conduct investigations at his own initiative or conduct on-site inspections.

14.8 The declaration requirement should apply to data used for journalistic purposes.