HONG KONG PLANS DATA PROTECTION LAW

Hong Kong would be the first Asian country to enact data protection legislation which applies to both the public and private sectors, if the recommendations of its Law Reform Commission's Privacy sub-committee are adopted.

When Hong Kong's government issued its *Data Protection Principles and Guidelines* in March 1988, it was presented as "an interim measure.....[with].....no legislative effect...[and] no enforcement or policing action to ensure compliance" (PL&B May 1988 pp.7,14). After two years experience, the government set up a Privacy sub-committee of the Hong Kong Law Reform Commission to formulate proposals for data protection legislation. The sub-committee's chairman, The Hon. Mr. Justice Barry Mortimer, explained the substance of the sub-committee's recommendations to the *Privacy Laws & Business* 4th Annual Conference in Cambridge and this report is an edited version.

Hong Kong, one of the world's leading financial centres, was the first territory in Asia to make any provision for data protection. In 1987 all the leading holders of financial data voluntarily accepted a code of practice broadly based upon the OECD Guidelines.

This is an excellent beginning but its limitations are recognised. Spurred by a determination to remedy shortcomings and the consequences of developing law in other parts of the world (particularly in the EC) a decision to legislate has been taken.

Some years ago a government working party to examine options was established but additional impetus came with the setting up of a sub-committee of the Hong Kong Law Reform Commission in March 1990 tasked to formulate proposals for Data Protection legislation. The contents of this paper offers the present thinking of the sub-committee and changes may be made in our final report. It goes without saying that whatever legislation is passed on this subject in Hong Kong is exclusively the concern of the legislature.

The Basic Approach

Having been presented with this challenge we seek to recommend a model law which will bear comparison with the best the world has produced so far. We are determined to propose a solution which suitably balances the legitimate interest of the data subject in his personal information with the public or commercial interest of the data holder in making proper and full use of the astonishing technology available both now and in the forseeable future.

We will propose, therefore, a model firmly based on principles of broad general application avoiding thereby a series of disjointed rules dealing with particular problems and providing the opportunity to build a coherent jurisprudence on the subject.

In addition to giving ourselves credit for some original thought we are drawing widely upon the laws and the practical experience of those working with them in many jurisdictions. It is a happy circumstance that as information technology transcends international boundaries so the relevance of the law transcends different legal systems. We are deriving great assistance from both common law and continental systems - with the balance in favour of the latter! Indeed, within the last few weeks Hong Kong has moved nearer to some of the continental EC countries by its enactment of a Bill of Rights which contains a right of privacy in the terms of the International Covenant on Civil and Political Rights. Against the public sector a right of action in tort is included. As in the Netherlands, Data Protection legislation may be regarded as putting flesh onto (others may say sense into) this skeletal semi-constitutional provision.

The Model (So Far)

The above approach led to important decisions:

That the law should have general application:

1. We proceed on the assumption (not made by other models) that the holding of personal data is near universal. They are (or soon will be) held by all businesses and organisations and by many individuals.
2. We see no reason either in practice or in principle to distinguish between data holders in the public and the private sector. Both will be subject to the law.
3. We propose that both electronic and structured manual records should be regulated. We cannot find any sound reason for not covering structured manaul records. It is impractical and unnecessary to cover unstructured manual records as they pose little danger to the data subject and it would be both unnecessary and unjust to regulate data of which the holder is unaware and cannot readily access.
4. We recognise that the advance of machine reading technology may soon erode this limitation.

That the law should broadly follow the OECD Guidelines:

1. For the avoidance of doubt we propose that provision is made for the erasure or destruction of personal data once the purpose for which it was collected and/or later held has gone. (But we note the possible interest of historians and archivists which we have yet to consider).
2. Subject to certain necessary exemption the general application of these broad principles will avoid the necessity for some of the detailed provisions found in other models. However, we are to give further consideration to the applicability of these provisions to certain types of data holder - for example:
   (i) Those who hold and process data for others.
   (ii) Those who collect and hold data for the purpose of transfer to or access by others.
   (iii) Those who collect on the same database a 'file' for a number of different purposes.

That a Data Protection Authority should be established:

The general purpose of the DPA will be to advise, formulate policy and monitor compliance with the law. We have made detailed decisions but it is enough to say that the DPA will consist of a Board of appointed, independent, part-time members. This will formulate policy. An independent Data Protection Commissioner will be responsible to the Board. He will have a suitable secretariat and his particular function will be to monitor compliance. He will receive complaints with powers of investigation, audit and decision. He can initiate enquiry but application to the court will be necessary to allow entry, or seizure or to order disclosure.

Upon receiving a complaint the Commissioner will decide whether a breach of the law is established. His certificate will be conclusive evidence of the facts upon which the Court will decide the scale of damage. Damages for injured feelings will be awarded.

Decisions of the Commissioner will be subject to appeal to a specialist tribunal. Judicial review of the decisions will be available.

To facilitate compliance and monitoring we also propose:

1. That every data holder must appoint a 'responsible officer'. He will be responsible (with the legal entity which controls the database or file) for compliance.
2. That every data holder should be required to furnish an annual declaration to the DPA briefly

describing the type of data held, the purpose for which they are held and the system under which they are held. This declaration will be on a form which has to be further considered. In this we aim for brevity and simplicity.

Further important matters

'Sensitive' Personal Data: I have not mentioned 'sensitive' data because we find no reason to differentiate between different types of personal data. We believe all personal data is potentially sensitive according to the particular circumstances of the data subject and his culture.

Personal Identification Numbers: Every citizen in Hong Kong has an identity card and a number. This is not a so-called 'smart' number.

In spite of original assurances to the contrary the number is widely used in both public and private sectors - often routinely and without apparent good reason. This is tolerated as an easy and effective means of establishing identity in a society where pseudonyms are common and numerous people have the same family name. Also the value of the identity card in maintaining a high standard of public order and safety is recognised.

To change this would not be possible (or advisable) but the proposed law would control the use of the numbers. The increased ease of computer matching is recognised but if lawfully undertaken the results will be more accurate.

Computer Matching: Computer matching (including the matching or assessing of data on the same database collected for different purposes) has recognised dangers for the data subject. Equally if appropriate and accurate it may produce legitimate public or commercial benefits. Some computer matching may be within the proposed law, other programs will not but may still be appropriate and proper. To accommodate this proper need the Data Protection Commissioner may approve and legitimate a matching program upon prior application. His discretion will be wide but will be exercised upon criteria specified in the law which will seek to ensure matching has a proper public or commercial purpose, is based upon accurate complete and appropriate data and that the identification of the subject is achieved. (We note the dangers. In Norway even with the use of 'smart' PINS there is still significant error in identification).

Additionally where an adverse decision upon a subject is contemplated after matching he will have the opportunity to check for accurancy and then correct the data.

Sectoral Codes: The Data Protection Commissioner will have the power and the duty to encourage the establishment of sectoral codes which may receive his approval. Following an approved code will not guarantee legality but will be a matter which the Commissioner, the appellate tribunal and the Court will take into account in any proceedings. The Commissioner may not therefore sanction a breach of the law.

Matters remaining for our further consideration:

1. Exemptions - total or partial
   - National security, defence, police records, etc.
   - Confidential reports - medical reports, etc.
2. Data holders who collect and hold data for the purpose of transfer or publication or access by others.
3. Data holders who hold and process data for others.
4. Data users who have 'on line' access to a data base held by another.
5. Commercialisation of data held.
6. The interest of historians or archivists in data to be erased or destroyed.
7. Transborder transfer

We have yet to consider this but it is likely that the sub-committee will seek to apply the same principles to transborder transfer as to any other transfer to third parties with the proviso that transfer will not be permitted to jurisdictions which do not have appropriate data protection laws. Each jurisdiction will be specified in subordinate legislation.

Consideration will be given whether to recommend that the Commissioner should have power to approve specific transfers.

Conclusion

We hope that the final model will achieve our original aim of balancing the proper interest of the subject with the public or commercial object of the holder so that the latter may continue to take proper benefit from present and future technology. We trust our model will also be both enforceable and sufficiently flexible and that no other jurisdiction will have any hesitation in exchanging personal data with Hong Kong.

The Hon. Mr. Justice Mortimer would welcome comments on the above proposals which may be sent to him via the *Privacy Laws & Business* office.

The Hon. Mr. Justice Barry Mortimer is a Judge at Hong Kong's Supreme Court and Chairman of the Hong Kong Law Reform Commission's Privacy sub-committee. He acknowledges the assistance given in the preparation of this paper by Mr Mark Berthold, Secretary to the Privacy sub-committee, and Mr Con Conway of Hong Kong Telecom, a member of the sub-committee.