How to comply with Hong Kong's data protection law

The Personal Data (Privacy) Ordinance was enacted in August 1995. Following the setting up of the Office of the Privacy Commissioner, the law was brought into force on 20 December 1996 (PL&B May '97 p.17). Data transferred to Hong Kong from other jurisdictions will generally become subject to the requirements of the Ordinance. To help organisations comply with the Hong Kong law, Mark Berthold, former legal advisor to Hong Kong's Privacy Commissioner, compares its main provisions with those of the UK Data Protection Act.

Sources of the Hong Kong Ordinance

The Ordinance has drawn its provisions from a variety of sources. The main ones referred to in this report are the UK Data Protection Act, the Australian Privacy Act, the New Zealand Privacy Act, and the European Union Directive Data Protection Directive. Accordingly, some of the provisions of the Ordinance will be more familiar than others. Essentially the Ordinance endeavours to reconcile comprehensive and rigorous protection of data privacy with due recognition of the demands of administrative and business practice whilst avoiding unnecessary bureaucracy.

The Hong Kong law and the UK Act compared

Short title: Unlike the UK Act, the short title of the Ordinance expressly states that it is "to protect the privacy of individuals in relation to personal data." This is significant because it facilitates a purposive interpretation of its provisions in accordance with the common law rules of statutory interpretation. An example of the practical relevance of the short title is provided by the decision of the House of Lords in *R. v. Brown* (PL&B Apr 1996, p.4-5) where a narrow majority held that the simple retrieval of data did not constitute "use" in the absence of its further deployment. However, in coming to the opposite view, the minority judgements concluded that a broader interpretation was necessary to protect the privacy of data subjects. In view of the short title, "use" under the Ordinance should be interpreted to accord with the minority decision in *Brown* (This is also the approach adopted by the Australian Privacy Commissioner).

Terminology: The Ordinance generally employs similar terminology to that of the UK Act. However, more of the relevant vocabulary has been expressly defined in section 2. Examples are "use" which is defined to *include* transfer or disclosure and data subject consent which is defined as "the express consent of a person given voluntarily."

Jurisdiction: As under the UK Act, the test of whether a person is a data user is determined by whether it *controls* the data. Generally speaking, foreign based organisations will be transferring data to their Hong Kong based subsidiaries or other Hong Kong data users. The application of the Ordinance's requirements to personal *data* is effected through the powers of the Hong Kong Privacy Commissioner and courts in respect of *data users*. The Ordinance will, therefore, be fully effective in these situations. However, where the data user controlling the processing in Hong Kong of personal data itself operates from another jurisdiction, there will be practical as well as jurisdictional difficulties in enforcing the requirements of the Ordinance.

Scope: The scope of the Hong Kong law is much broader than that of the UK. It covers all personal data "in a form in which access to or processing of the data is practicable" (s.2). Accordingly, not only computerised records but also organised manual records are covered. *Data* is defined as "any representation of information (including an expression of opinion) in any document" and *document* includes media for the recording of visual and audio data. Accordingly, staff records and other documented assessments held manually are subject to the Hong Kong law.

The data protection principles

The core of all data protection laws is a set of data protection principles regulating the collection, use, quality, and security of personal data and providing the data subject with the legal right to access and correct such data. As with the UK Act, these principles are set out in Schedule 1 of the legislation. Their formulation differs somewhat from those of their UK counterparts.

Fair collection: Principle 1 of the Ordinance replicates the UK requirements that collection be

lawful and fair. However, collection pursuant to another enactment is not necessarily deemed to satisfy this requirement. Furthermore, the Hong Kong provision requires that data users shall only collect data for a lawful purpose which is directly related to their functions or activities. The collection must be necessary for or directly related to that purpose. The purposes of the data user is a question of fact and is not determined by a registration entry as under the UK scheme. It would not be permissible, for example, for a clothing shop to collect data on a customer's health.

Furthermore, the Hong Kong formulation stipulates certain matters that the data subject must be expressly informed of when collecting data, namely data purposes and the classes of transferees. He must also be made aware of whether providing the data is voluntary or obligatory and the consequences of not providing them. However, where this will be obvious from the context, it need not be made explicit. The data subject must also be expressly advised of access and correction rights and the necessary contact details for effecting these before the data is used.

Use limitation: Hong Kong's Principle 3 provides that personal data shall not be used for any purpose "other than the purpose for which the data were to be used at the time of the collection of the data" and these may be called the *prescribed purpose*. Whereas data purposes are determined by the UK registered entry, the Hong Kong law imposes a factual test. The most useful test to determine the prescribed purpose is that of the reasonable expectations of the data subject. Where the data purposes have been stipulated upon collection, then these will determine those expectations, otherwise it will depend on the functions of the data user and the surrounding circumstances. This approach is necessarily less cut and dried than that of the UK.

A departure from the prescribed purpose is only permitted by the Ordinance where either the data subject has given his consent or a relevant exemption applies. It has to be admitted that this does result in some rigidity. For example, it may not be possible to contact data subjects to seek their consent. Also, consent must be express. It is not, therefore, permissible for a data user to advise its customers that it proposes altering the purposes for which data will be used unless the data subject objects. Implied consent is not sufficient under the Ordinance.

Data quality: Whereas the UK Act defines *inaccurate* as "incorrect or misleading" the HK definition extends to "incomplete or misleading" data. More fundamentally, the accuracy requirement is not expressed as an absolute but is determined having regard to the data purposes. So archival data is not obsolete in view of its purpose.

The Hong Kong law goes further than the UK Act in requiring that where it transpires that a data user has disclosed inaccurate data, it must remedy this by providing the recipient with corrections.

Data security: This is similar to the UK requirement, although it spells out more explicitly the factors relevant in determining the stringency of security safeguards to be employed.

Access and correction rights

These are spelt out in much more detail by the Hong Kong law and generally provide the data subject with greater protection. Whereas the UK Act enables a data subject to go to court to order a recalcitrant data user to correct personal data, in Hong Kong, the data subject may complain to the Commissioner who may issue an enforcement notice requiring the correction.

As with the UK law, personal data includes "an expression of opinion." However, diverging opinions may be legitimately held regarding the same matters with neither necessarily being incorrect or misleading. Accordingly, the Hong Kong law provides a mechanism whereby the data subject may have appended to his data a note stating his viewpoint where the data user is not satisfied that his own opinion on the matter is "inaccurate."

Whereas all the provisions of the Ordinance (except those regarding matching and transfers out of Hong Kong mentioned below) were brought into force on 20 December 1996, a one year transition period is provided regarding the correction of data. This means that until 19th December 1997, in response to a data subject's access request, a data user may give a data subject a cleaned up record, but must say so.

The law gives no guidance on an access fee. But the intention of the law is that one access fee

should be paid for all data held by the data user. The data user may insist that the fee is paid in advance, otherwise, the access request may be refused. If an access request is refused for any reason, that refusal must be recorded in a log book and held for four years.

Regarding language, the law says that a request in say, Chinese, must be answered with the data in Chinese, if the data user has the data held in that language. Likewise, for a request in English. However, if the data is *not* held in the language of the request, there is no legal requirement to translate the data into that language.

Registration

The Ordinance does not itself impose any notification requirements on data users. Instead it empowers the Commissioner to designate classes of data users who must notify him of the basic features of their data holdings. Even then, unlike under the UK Act, the requirement is purely that of notification rather than registration, as the Commissioner's consent is not required for processing. To date, the Commissioner has not designated any classes of data users and it is expected that he will proceed selectively. Notified matters, (such as purposes and transferees) will be available on-line to data subjects and will promote transparency as well as facilitating the Commissioner monitoring designated sectors. A prime target is, accordingly, likely to be those data users which provide reference services to other data users by pooling data collected without the involvement or knowledge of data subjects.

Codes of practice

Unlike the UK Act, the Ordinance expressly recognises the role of codes of practice. The role of codes is that of "providing practical guidance" regarding the requirements of the Ordinance. A code lacks the legal status to qualify or amend these statutory requirements, including the principles. On the other hand, to be useful a code should go further than an arid repetition of these requirements.

With two exceptions, the Commissioner has indicated that it is up to the various sectors to do the initial work developing their codes. The first step is the preparation of guidelines which are scrutinised by the Commissioner's office. These provide the basis for draft codes. Before approving the code, the Commissioner is required to consult the relevant sector and other relevant persons. Upon approval, the code is gazetted. Failure to comply with a provision of a code does not itself render the data user liable to civil or criminal proceedings. However, in proceedings to establish whether a statutory contravention has occurred, a breach of a relevant provision of a code will be treated as *prima facie* evidence of the contravention.

The two areas where the Commissioner has to date taken the initiative is developing codes are *credit data* and *personal identifiers*. Codes on both these issues should be approved by the year's end.

Data matching

It is increasingly recognised that the comparison of personal data collected for different purposes to identify discrepancies and take adverse action is an invasive investigative technique that warrants special safeguards. Sections 30-33 accordingly regulates "matching procedures," the definition of which derives from the New Zealand Act. The Commissioner's consent is required, except in the unlikely event that all the subjects of the matching exercise provide their consent. Nor may adverse action be taken regarding "hits" without providing an opportunity to contest the results. *Matching procedure* does not encompass profiling which does not involve the *comparison* of data. These matching provisions are likely to be brought into force before the end of the year and in anticipation of this, some 17 applications have already been received by the Commissioner.

Direct marketing

Section 34 derives from a requirement of the European Union Data Protection Directive and requires that upon the first use of data for direct marketing purposes, the data user must inform the data subject that upon his so requesting, it shall cease to use that data. The Hong Kong Direct Marketing Association advises its members that it should include this opt-out statement with all marketing approaches. This is because the requirement is expressed to apply to the first use of "*those* data" and hence will apply whenever the data have been enhanced. Under the Ordinance *use* extends to simple retrieval of data.

As the opt-out requirement does not address the situation where the data user does not itself have control of the data (for example, because it has used labels provided by a list-broker), the Association also advises that it should relay opt-outs to the source of the data. This constructive suggestion is aimed at preventing data subjects from becoming unnecessarily frustrated at lack of follow-up on their opt-outs. Due to the inertia effect, only a small number of opt-outs are being received.

Transferring data from Hong Kong

Section 33 regulates the transfer of personal data out of Hong Kong. As with the matching provisions, it has not yet been brought into force. Nor is that imminent. The Commissioner may well await the lead of the European Union in determining which jurisdictions possess laws which provide sufficient protection, notwithstanding that s.33 provides an equivalence rather than an adequacy test. Like the EU provision which it is based on, s.33 permits transfers to jurisdictions lacking a data privacy regime where the interests of the data subject are otherwise adequately protected. Examples are where the subject's consent has been obtained or the transferee has obtained the transferee's contractual assurances that the data protection principles will be respected. The Commissioner has already issued a draft contract based upon that of the Council of Europe. Transfers are also permitted which accord with one of the specified public interest exemptions summarised below.

Exemptions

Like the UK Act, the Ordinance prescribes a number of exemptions from the access requirements and/or use for an altered purpose. However, the Hong Kong exemptions scheme is more extensive than the UK one. This is a corollary of the Ordinance's application to cover not only computerised data but also retrievable manual data. Accordingly, access exemptions are available to employers regarding their staff planning records and references, as well as a transitional provision for data provided in confidence.

The exemptions also extend beyond law enforcement to "the prevention, preclusion, or remedying of unlawful or seriously improper conduct." This expression also encompasses the maintenance of ethical and professional standards including those whose breach may warrant disciplinary proceedings.

Various elaborations are also provided to facilitate the role of financial regulators. There is also an exemption provided regarding news which has been carefully crafted to balance the rights of data subjects with the role of the free press. Features of this exemption include a *whistleblower* provision protecting sources and the exclusion of access to unpublished journalistic data, including a journalist's notebooks. The legislature was satisfied that to provide data subject access to unpublished data could stymie journalistic enterprise. These provisions would repay close study by those responsible for amending the UK Act to bring it into line with the EU Directive.

Commissioner's powers and procedures

Like its UK counterpart, the Hong Kong Privacy Commissioner may investigate complaints alleging contraventions of the legislation. Applicable procedures impose greater accountability than under the UK Act. For example, strict time limits are imposed requiring that within 45 days of receipt of a complaint, the Commissioner must either formally investigate or advise the data subject why it is refusing to investigate and advising him of his rights or appeal. There is also provision for the publication of reports which may identify errant data users. To date, one report has been issued. It relates to the surreptitious videotaping of a female student in a dormitory. However, the Commissioner's Office contents itself with a mediation role where a mutually satisfactory outcome is achievable.

To date, the vast majority of complaints received relate to the private sector. The data protection principle that has elicited most complaints is the finality principle requiring that data should not be used for a purpose other than that for which its was collected without the data subject's consent.

In addition to this reactive role, the Commissioner is also empowered to institute investigations at his own initiative where he reasonably suspects a contravention. He may also institute inspections which are similar to the audits which his counterparts in Australia and Canada may conduct. To date, the Commissioner's

modest resources have precluded any inspections being conducted as they will require the assistance of management consultants. The Commissioner's proactive powers of investigation and inspection do not extend to news organisations. This is to better preserve the institutional integrity of the press.

The Ordinance has appropriated from the UK Act the mechanism of enforcement notices. However, an enforcement notice may be issued in respect of *any* contravention, provided it is either continuing or likely to repeated. As the Ordinance does not impose a registration requirement, there is no provision for de-registration notices. Non-compliance with an enforcement notice is, however, a criminal offence. Accordingly, no matter how recalcitrant a data user may be, he may continue to process personal data.

Offences and compensation

Like the UK Act, the Ordinance neither requires nor assumes that disgruntled data subjects must seek assistance from the Privacy Commissioner. However, rights of redress are more extensive under the Ordinance. Compensation may be claimed in court or the Small Claims Tribunal for any contravention of the Ordinance by a data subject who has suffered damage thereby, including injury to feelings. It is a general defence that the data user has taken reasonable care to avoid the contravention. Whereas employers and principals are vicariously liable for an act or practice engaged in by employees or agents, liability is avoided where reasonably practicable steps were taken to prevent the offending act or practice.

An admittedly odd feature of the Ordinance is that a contravention of *any* provision of the Ordinance, other than one of the principles, is a *criminal offence*. The Commissioner has no discretion *not* to refer an apparent offence to the prosecuting authority. However, he must be reasonably satisfied that an offence has occurred. Private prosecutions are another possibility.

One of the consequences of the Ordinance's extensive use of criminal sanctions is that the privilege against self-incrimination is of much greater potential significance than under the UK Act. An individual will wish to invoke this privilege where the Commissioner is seeking information that may lead to his conviction under the Ordinance. However, the Ordinance focuses on the culpability of *data users* (i.e. organisations) and usually the acts or practices of individuals are only relevant to the extent that they establish the culpability of the organisation. Accordingly, the privilege will not be relevant to lower level employees whose acts have contravened the Ordinance. Where it will be relevant is where the individual was acting as part of the directing mind of the company because, as under the UK Act in these circumstances, *personal* liability attaches.

Conclusion

The Hong Kong Ordinance differs from the UK Act in a number of significant respects. As the Ordinance's generally more robust protections reflect several of the requirements of the EU Directive, it is likely that the amended UK Act will more closely resemble the Ordinance than the present Act.

This paper is based on a presentation given in London on August 21st by its author, Mark Berthold, BA LLB., Barrister and Solicitor. He is an independent consultant, who was Secretary to the Hong Kong Law Reform Commission committee which provided the basis for the bill. He subsequently was the legal advisor to the team which drafted the law. Following the enactment of the legislation, he has been the principal legal advisor to Hong Kong's Privacy Commissioner for Personal Data.

His contact address is GPO Box 3434, Hong Kong. His UK contact office is at *Privacy Laws & Business*.

He is the co-author of *Data Privacy Law in Hong Kong*, published by FT Law & Tax Asia Pacific. Tel: + 852 2863 2659 Fax: + 852 2520 6954. HK $595/US $108.
ISBN: 9626610409.