COMMENT

■

Data Privacy: Reforming the Law

The Personal Data (Privacy) Ordinance[1] will have a major impact on the way in which information is collected, stored, and transferred. Personal information about us will be accorded significantly greater protection than has ever been the case. Of the three cheers to be raised, at least one belongs to the process that yielded this important piece of legislation. I shall suggest why below.

The ordinance (most sections of which are expected to come into force before the end of this year) provides individuals with comprehensive safeguards against the misuse of personal information and a right of access to it. The scope of the statute is plain once it is realised that 'personal data' is broadly defined to mean any data relating to a living individual from which it is practicable for his or her identity to be ascertained. Even though this is restricted to data in a form in which access to or processing of the data is 'practicable,' the reach of the law is long.

The protection of personal data is a delicate and difficult subject that touches on almost every aspect of our lives.[2] Not only does it represent a classic instance of the law's struggle to keep abreast with science, but the rapid advances in information technology have spawned problems that test the ability of the law to provide adequate protection against abuse. Data protection is merely one. The routine functions of government and private institutions require a continual supply of data about us in order to administer effectively the many services that are an integral part of modern life. The provision of health services, social security, credit, insurance, and the prevention and detection of crime assume the availability of a considerable quantity of personal data and, hence, a willingness by individuals to supply it.

The ubiquity of computers and computer networks facilitates, of course, almost instant storage, retrieval, and transfer of data, a far cry from the flat-footed world of manual filing systems. These developments are sometimes decried as the nemesis of whatever vestiges of privacy still survive. In respect of the future of privacy, at least, there can be little doubt that the questions are changing before our eyes. And if, in the domain of atoms, we have achieved only limited success in protecting individuals against the assaults on their privacy, how much better the prospects in our binary universe?

Hong Kong has at last caught up with the nearly thirty jurisdictions that have introduced data protection legislation in an effort to regain some of this lost ground. Most of these statutes draw on the provisions of the OECD guidelines of 1981 and those formulated by the Council of Europe in 1980. Last

1 Ordinance No 81 of 1995.
2 See Raymond Wacks, *Personal Information: Privacy and the Law* (Oxford: Clarendon Press, 1993), pp 178–245.

HeinOnline -- 26 Hong Kong L.J. 149 1996

year the European Union adopted the European Directive on Data Protection which provides a comprehensive framework binding on member states. They have three years to implement its provisions.

Hong Kong's Bill of Rights Ordinance in s 14 gives effect to Art 17 of the ICCPR which provides for the protection against 'arbitrary or unlawful interference with ... privacy ...' This has been interpreted by the United Nations Human Rights Committee to include data protection. In the same year the UN General Assembly adopted guidelines for the regulation of computerised personal data files. Articles 29 and 30 of the Basic Law of the Hong Kong SAR contain general declarations of support for 'privacy' that might be construed as embracing the protection of personal data.

None of this adds up to very much. It is therefore to the credit of the Law Reform Commission of Hong Kong that in October 1989 a sub-committee was established to examine whether the law needed to be beefed up. The sub-committee (of which I am a member) reported in August 1994.[3] Two months later the Governor announced that legislation would be introduced. Broadly speaking, the ordinance adopts the many recommendations of the Law Reform Commission.

Two conspicuous features distinguish our legislation from most similar statutes elsewhere. First, it applies both to computerised and manually held data. Second, it extends both to the public and private sectors. At the heart of the new data protection regime is the concept of fair information practice: in particular, the proposition that data relating to an identifiable individual should not be collected in the absence of a genuine purpose and the consent of the individual concerned. At a slightly higher level of abstraction, it encapsulates the principle of what the German Constitutional Court has called 'informational self-determination'[4] — a postulate that expresses a fundamental democratic ideal. It is hard to overstate the importance of the 'use limitation' and 'purpose specification' principles as canons of fair information practice.

Adherence to, or more precisely enforcement of, this idea (and the associated rights of access to one's personal data and correction of errors) has been mixed in those jurisdictions that have enacted data protection legislation. It is to be hoped that the new Privacy Commissioner for Personal Data (whose powers are not inconsiderable) will quickly create an environment in which these principles are widely adopted and effectively enforced.

The enactment represents an exemplary process of law reform, particularly in the light of current circumstances in the territory. The process which culminated in the legislation is instructive. Sub-committees appointed by the Commission generally appear to represent a coalition of interest and expertise,

3 *Report on Reform of the Law Relating to the Protection of Personal Data*, Topic 27 (Hong Kong: The Law Reform Commission of Hong Kong, 1994).

4 *Volkszahlungsurteil* (National Census Case) (1983) 65 BVerfGE 1, 68-9, cited in S Simitis, 'Reviewing Privacy in an Information Society' (1987) 135 University of Pennsylvania Law Review 707, 734.

HeinOnline -- 26 Hong Kong L.J. 150 1996

and, as far as one can tell, an attempt is made to provide a 'cross-section' of the community. This approach is easy to deride. But on this occasion at least, the result was a satisfying one. Serving as a member of a sub-committee is time-consuming, unpaid work. The group met 56 times and, despite the controversial nature of the subject-matter, a consensus emerged on all major questions. The consultation paper was unanimous in its proposals.

The Commission is not an independent body; it resides within the Legal Department, and its chairman is the Attorney General. Though this may suggest a conflict of interest, or at least a confusion of functions, it plainly enhances the prospects of the Commission's proposals being translated into law, as occurred with spectacular speed in this case.

Another remarkable feature of this experience was the extensive consultation exercise conducted by the sub-committee. This included numerous seminars held by interested organisations such as the Consumer Council, the Journalists Association, the Society of Accountants, the Association of Banks, and the Direct Marketing Association. During the consultation period some eighty submissions were received (and required the sub-committee to meet another twenty times for them to be considered). That the overwhelming majority of responses supported the proposals does not mean that when the law begins to bite it will be painless. Compliance with the ordinance will require far-reaching changes in current attitudes and practices of information management. This is bound to generate expense and irritation. Hong Kong's non-interventionist culture, particularly in the business sector, is in for a jolt. For most 'data users' the law will intrude upon virtually all stages in the collection and use of personal data. The right of 'data subjects' to obtain access to and correct erroneous data about them will, when it comes into force, have a profound effect on record-keeping and confidentiality. The Privacy Commissioner will need to be both constable and educator.

The enactment of this ordinance and the existence of similar legislation in several jurisdictions in the region (Japan, Taiwan, New Zealand, Australia) or recent proposals to introduce data protection laws (Singapore, South Korea) are driven only partly by altruism. The new information technology disintegrates national borders; international traffic in personal data is a central feature of commercial life. The protection afforded to personal data in Country A is, in a digital world, rendered nugatory when it is retrieved on a computer in Country B in which there are no controls over its use. Hence, states with data protection laws frequently proscribe the transfer of data to countries that lack them. Indeed, the European Directive explicitly seeks to annihilate these 'data havens.' Without our new ordinance, Hong Kong would risk being shut out of the rapidly expanding information business. And, with an increasing quantity of data moving between Hong Kong and China, how long can it be before the PRC will need to adopt similar legislation?

Raymond Wacks

HeinOnline -- 26 Hong Kong L.J. 151 1996