Data Protection Legislation in Hong Kong: A Practical Perspective

EVA Y.W. WONG

CITY POLYTECHNIC OF HONG KONG

ABSTRACT

Hong Kong is an important financial, commercial and industrial centre in the rapidly developing Far East region and information technology (IT) is used extensively in both the private and public sectors. Unlike many western countries, there are presently no explicit information technology laws in the territory. However, the Hong Kong Government is seriously considering legislation in this area. This paper examines current data protection practices in the territory, discusses the issues raised in a recently published consultative document, and deliberates the implications of data protection legislation for those doing business in Hong Kong.

INTRODUCTION

Many organizations, in both the private and public sectors, have been dramatically transformed by information technology [23,24,34]. An important change is the capability to electronically store tremendous amounts of personal data and information. As a result, businesses around the world now face a serious dilemma: although the use of computer-based information systems (IS) has created new business and service opportunities, these systems also invite the computer hacker and the criminal [26].

Computers pose a potential danger to individual privacy [6,11,32,33]. They are able to store vast amounts of data, have the facility to process and transfer these data at high speeds, and the further capability to correlate across data sets. Advancements in information technology (IT) have also lead to the re-evaluation of ethical principles and practices [17,29]. Society has had little time or experience in developing appropriate ethical concepts and dealing with privacy issues, since computer science and technology have been and still are fast advancing.

Moreover, data communications take place without personal contact, changing relationships between people. Information held in electronic, magnetic, and optical form is more prone to unauthorized alterations and access, and is far more fragile than information held on paper. Although computer users expend considerable effort in protecting the integrity, confidentiality and availability of computer-stored information, there has been limited consideration of ethical and privacy matters [17,29].

The potential threat of IT to individual privacy and the ethical issues related to computer use have led many Western countries, like the United Kingdom (UK) and the United States (US), to establish data protection legislation. These laws control the collection, storage, use and disclosure of personal data by means of computers and telecommunications techniques [1,15,25,37,38]. The recent explosion of IT use in Hong Kong (and more generally Asia) combined with the lack of legislation to protect data or individual privacy raises an important question: Are the interests of business and society adequately safeguarded?

This paper looks at the current data protection situation in Hong Kong, and examines the proposals in a recently published consultative document [18]. Furthermore, if data protection legislation as suggested by the document were implemented, what would organizations and businesses have to do to comply? The implications of a data protection law for businesses and organizations in Hong Kong are discussed.

Hong Kong is an important business center for the Asia-Pacific region. Its pragmatic use of IT has effectively leveraged human resources and stimulated remarkable economic development [21]. By discussing the current and projected data protection status for Hong Kong, this paper seeks to put the Hong Kong situation into a global context. It is shown that implementation of a data protection law would serve both public and business interest while preserving Hong Kong's international reputation.

The Current Status of Data Protection in Hong Kong

There is no data protection legislation in Hong Kong at present. In March 1988, the Hong Kong Government published a document entitled "Data Protection Principles and Guidelines" [10]. This document aimed to provide general guidance on data protection in order to preserve the confidentiality of computer-based personal data while enabling IS users to collect, store, use and disclose personal data in a proper manner. Although government departments and private businesses were encouraged to follow the principles and comply with the guidelines, the document has no legislative power [10].

In Hong Kong, large amounts of personal data are already being held and processed on computers in assorted organizations. Without proper data protection laws, there is a heavy reliance on the good will and professional ethics of computer users. Individuals presently have no legal rights to check that their records on computers are correct, accurate and up to-date. In fact, people (and businesses) do not even have the right to access their own computerized records. Furthermore, if data is found to be incorrect, there is no proper channel for complaint. Unscrupulous computer users who intentionally misuse computerised personal data are not directly liable for a criminal offence. This situation is a significant business and social concern in Hong Kong [4,18,19].

As a major international financial and commercial center, there is an enormous volume of transborder data flow (TDF) in and out of Hong Kong [11]. Such data may be stored and re-processed in a country other than the originating country. TDFs stem from airline reservations and credit card transactions as well as electronic funds transfers [11]. The need to safeguard personal or company data from being illegally transferred across political borders, to protect security interests or individual rights, has prompted TDF regulations.

Several countries which signed the Council of Europe Convention on Data Protection [7] have enacted specific TDF legislation. It prohibits TDFs to those countries or territories which are not signatories to the Convention, where the flow is likely to lead to a contravention of the Convention's data protection principles. Recent publications [8, 12, 13, 14, 15, 26] reflect the growing concern about privacy in the developed countries. As a result, exchanges of personal information, even between countries having data protection laws, such as Western European countries and the United States, are being affected [31].

Technological advances have globalized data protection and privacy issues [22]. Legislation enacted in one country is capable of affecting trade and business with its partners [31]. Hong Kong's position as a financial and commercial center could be jeopardized. Countries with data protection laws may restrict the flow of personal data to the territory because of the absence of such legislation in Hong Kong. Thus, data protection legislation may be critical for the future well-being of both people and businesses in Hong Kong.

The 1997 transfer of political sovereignty from Britain to China provides another reason for the establishment of data protection legislation in Hong Kong. China does not have and is unlikely to soon enact such legislation. In Hong Kong, a new Basic Law will come into force in July 1997. Only one part of this law, Article 30, even remotely deals with the data protection issue, addressing the freedom and privacy of communication [12].

There are two important reasons to implement a data protection law before 1997. First, it will promote the continued prosperity and stability of Hong Kong, and help maintain the territory as an international business hub. Second, at some stage of its socioeconomic development, China will also need to establish data protection legislation. The Hong Kong experience can then be used as a model.

Given this situation, the Hong Kong Government is belatedly considering laws to govern protect data and individual privacy. In March 1992, a Bill on Computer Crimes was published, for the first time, in the Hong Kong Government Gazette [5]. This Bill introduces new types of criminal offenses for activities involving the use of computers. In particular, the Bill addresses issues related to computer fraud and computer abuse. Under the Computer Crimes Bill, four new offenses are being introduced by amending the existing criminal code relating to telecommunications, crimes, and theft. These offenses cover unauthorized access, unlawful tampering with computers, programs, or data, accessing a computer to commit further crimes, and trespassing with intent to tamper with computers, programs, or data [19]. This is intended as a prelude to IT-related laws in Hong Kong. It signals that the Hong Kong Government is finally ready to tackle this complicated area. Perhaps more importantly, the Bill is among the first of its kind in the rapidly developing Far East region [18]. Regrettably, this Bill does not cover data protection issues.

In March 1993, the Privacy Sub-committee of the Law Reform Commission of Hong Kong published a consultative document which deals extensively with matters concerning data protection and privacy [18]. The recommendations are based on the Organisation for Economic Co-operation and Development's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [27]. Since future data protection legislation in Hong Kong will be based on it, further examination of these recommendations is appropriate.

Information Privacy Law Reform

The rapid growth in computer use and the swift advancement in related technologies prompted the establishment of the Privacy Sub-committee to study data protection is-

sues. This sub-committee made a detailed study of the OECD Guidelines and based its recommendations on them. In addition, principles underpinning the Convention and the European Communities Commission's amended proposal (the draft Directive) [3] were also examined by the Sub-committee to provide useful references.

The document details the eight data protection principles identified by the OECD Guidelines and makes recommendations as to how new legislation should resolve matters in breach of the principles. The principles are very general in nature and mainly concerned with good practices. In addition to covering the conduct and responsibilities of data users, they specify the security measures which must be installed to safeguard data integrity and accuracy, and to protect them from unauthorized alteration or destruction. Data transfer, disclosure, access and verification procedures are also clearly defined by these principles.

The sub-committee recommends giving new rights to individuals whose personal data is recorded in a computer-based environment. They may find out what data has been recorded, challenge its accuracy and claim compensation if they have been affected by wrongly recorded information. The document suggests obliging data users to collect, store, use and disclose personal data only in a manner that is lawful, proper and fair to the data subjects. Every personal data holder would have to furnish a public declaration to the Privacy Commissioner, thereby enabling the public to know about the data being collected and its use. Due to the nature and purpose of this document, which is mainly for consultation, it stops short of specifying or identifying what constitutes a criminal offence.

An independent regulatory agency would, however, oversee data protection practices in Hong Kong. A Privacy Commissioner would be responsible for the following:

- publicising data protection laws
- promoting compliance with the data protection principles
- initiating and conducting on-site inspections of record keepers
- investigating complaints about breaches of the principles or the law, and
- enacting prosecution where appropriate.

A register of data users holding personal data would also be created. Everyone holding personal data on a computer must make a formal declaration to the Privacy Commissioner describing the data user himself, the data he holds or intends to hold, the purpose and use of the data, and the third party or parties to which information may be disclosed. In compliance with the OECD Guidelines, this registry would be accessible to the public. Data subjects could discover what is being held about them, by whom and for what purposes.

The Privacy Sub-committee proposals are intended to lead to the establishment of data protection legislation in Hong Kong. Such legislation would allow Hong Kong to become a party to internationally recognized data protection regulations. Without such ratification, the following are likely: constraints on the territory's international trade, rising information management controversy and declining public confidence in business computing.

The Hong Kong proposals are in line with internationally recognized data protection practices. Many Western countries already have data protection legislation in place. In the United Kingdom, the Data Protection Act of 1984 [9] deals with data protection matters. Many business activities there are affected by this act [1,25,35]. Organizations and individuals have to register their entries with the Data Protection Office and adhere to a set of data protection principles. Data integrity and accuracy is also subject to safeguards. Data subjects must be able to check that information about them is correct and up-to-date.

Several published booklets and an adjustment period from 1984 to 1987, were used to institutionalize this change. Compliance with the Act has increased administrative controls and functions and raised the cost of doing business [6,16,33,39]. However, it has helped to ensure the free flow of personal data across the borders of the United Kingdom and raised public confidence in respect of their records being held on computers [12,13,25,26].

Implications of a Data Protection Law

If a data protection law is introduced in Hong Kong, data users will have to make explicit written declarations to the data protection authority. Data could then only be used for the fulfillment of specific purposes, implying that a declaration should not and will not last forever. Organizations using personal data would also be responsible for setting procedures and promoting data protection practices [10,11,16]. Employees and agents of such firms would be bound to observe the terms of the data user's declaration. Even unintentional misuse or misunderstanding could make the data user criminally liable.

The Hong Kong Government has already advised organizations which need to adopt data protection practices to appoint a senior officer or a committee to assess, authorize, monitor and review, on a routine and on-going basis, data protection measures in existing and new computer applications [10]. In this respect, compliance with the data protection legislation not only increases the administrative and management duties of an organization, but it may also present the organization with related legal liabilities.

The data protection legislation will also require data users to implement proper security measures to guard against unauthorized access to, and alteration of personal data. These

measures should also be adequate and effective to protect the data from accidental or malicious loss or destruction. Only authorized users would be allowed to use and process the personal data; the accuracy and integrity of the personal data would be preserved; disclosure or transfer of the personal data would be legitimate. Considerable resources will be needed to implement compliance with the proposed law.

Private and public organizations will also have to respond to personal requests for subject right of access and correction. Computerised personal records must be available for data subjects if formal requests are made. As a result, firms will have to incorporate proper procedures to validate the request, authorize the access, issue the information and record the action taken. Matters arising from subject rights of access and correction are complicated. Additional explanation and guidance usually have to be provided if the procedures are to function effectively. In the United Kingdom, the Department of Health published additional guidelines and procedures for the National Health Service to deal with subject access to personal health information, to supplement the booklets printed by the Data Protection Registrar's office.

Declarations submitted to the Privacy Commissioner by each data user will describe whether the personal data will be disclosed to third parties, which may include the transfer of the data to another country or territory. A data user must consider the implications of any personal data disclosure or transfer. Such actions should not, under normal circumstances, cause harm or adverse effects to the data subjects. As Hong Kong is a free port, with people, merchandise, currencies and data flowing relatively freely into and out of the territory, the restrictions on personal data disclosure and transfer placed on organizations by data protection law may have wide-ranging repercussions.

Data protection legislation will inevitably create extra administration overheads for businesses [16,37,38]. In Hong Kong, this may deter private enterprise activity. However, firms from Europe or North America will already be familiar with similar data protection requirements. Existing data protection legislation in those countries is already likely to have required them to implement and maintain secure computer systems [16]. Such multinationals may even welcome data protection legislation in Hong Kong. Their local business rivals, with less experience in this area, could be at a competitive disadvantage.

In order to enforce its data protection legislation, an increase in government bureaucracy is also inevitable. Law enforcement agencies, such as the Hong Kong Police Force, or the Independent Commissioner Against Corruption (ICAC), will also have increased responsibilities [30]. However, growing public concern makes data protection legislation a regulatory necessity, despite the bureaucratic burden [6,22,38]. As Hong Kong businesses increasingly rely on IT, local law makers and law enforcement agencies have to address technology-related issues.

CONCLUSIONS

The Hong Kong Government has recognized the importance of having a data protection law in the territory [10,18]. However, implementation and enforcement will not be simple matters. Other countries have experienced an assortment of implementation enforcement problems [12,13,38]. The registration system of the United Kingdom's Data Protection Act has been criticized as being too complex and cumbersome. Many small businessmen are ignoring the registration requirement [4].

In view of these problems, the Hong Kong Government has undertaken a thorough examination of the different data protection laws which have been adopted and practised around the world. Its seeks to enact local legislation which is compatible with existing positive non-interventionist government policies and suitable for the Hong Kong economy, which is dominated by small and entrepreneurial businesses [10,21]. The consultative document by the Privacy Sub-committee represents the first step in this approach.

Although the Hong Kong Government is promoting good data protection practices in both its departments and in the private sector, the application of data protection measures is still all too often ignored [39]. When such practices are implemented, it is usually for reasons of profit protection rather than privacy protection. Despite attempts to assure the public that they can rely on the professionalism of data users to handle personal data lawfully, fairly, ethically and properly, such voluntary practices are neither effective or adequate.

Professional bodies like the Association of Computing Machinery (ACM) in the U.S. and the British Computer Society (BCS) in the United Kingdom have actively encouraged good practices among their members [28]. For example, the ACM has completed and published a revised Code of Ethics and Professional Conduct for its members [36]. However, as increasing numbers of people in widely diverse situations use computers, a professional code of conduct may not be observed by all, and disciplinary procedures remain inadequate [1,4].

The concept of data protection and its relationship with privacy is relatively new to most individuals and organizations in Hong Kong and the region [4,10,21]. New legislation in this area will transform, or at least alter, many business management practices [8,20]. Prudent managers operating across much of Asia will have to ensure that their organizations are registered and will have to notify the authority of any subsequent changes in the use of the personal data [35]. Individuals will have to be made aware that misuse of personal data, no matter how trivial, is an infringement of privacy

[18,28,29]. The Privacy Commission in Hong Kong, and similar authorities in other economies, will have to stress promotional, educational and publicity functions [18]. IS management researchers and practitioners can contribute by participating in the formulation of new legislation as well as developing and testing appropriate data protection policies and frameworks.

With the consultative document from the Privacy Sub-committee and the gazetting of the Computer Crime Bill, a data protection law may soon be a reality in Hong Kong. Although substantial resources will be needed to ensure enforcement of and compliance with the law, this will be well-spent time and money. Relying on the goodwill and professional ethics of data users or tackling this strategic issue in a piecemeal manner has done little to inspire public or business confidence [21,28]. Moreover, an effective regulatory framework in Hong Kong can serve as a model for China and other industrializing economies in Asia.

REFERENCES

[1] Andrews, D., "The Protection Man," *Credit Management,* June 1989, pp. 20-23.

[2] Chan, M.K. & Clark, D.J., *The Hong Kong Basic Law: Blueprint for "Stability and Prosperity" under Chinese Sovereignty?* Hong Kong University Press, 1991.

[3] Commission of the European Community. Amended proposal for a Council Directive on the *Protection of Individuals with regard to the Processing of Personal Data*, 1992.

[4] "Computers and Privacy," *The Economist*, May 4, 1991, pp. 19-20.

[5] *Computer Crimes Bill 1992,* Legal Supplement No. 3, Hong Kong Government Gazette, No.13, Vol. CXXXIV, 27 March 1992.

[6] Corbitt, T.D., "Security and Privacy of Information," *Credit Management,* February 1990, pp. 20-21.

[7] Council of Europe. Convention for the *Protection of Individuals with regard to Automatic Processing of Personal Data,* 1981.

[8] Culnan, M.J., "How Did They Get My Name?: An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use," *MIS Quarterly,* Vol. 17, No. 3, September 1993, pp. 341-361.

[9] *Data Protection Act 1984,* Guidelines 1-8, United Kingdom, February 1989.

[10] *Data Protection Principles and Guidelines,* Government of Hong Kong, March 1988.

[11] Edwards, C., Savage, N. & Walden, I., *Information Technology and The Law,* Macmillan, 1990.

[12] Ellis, S. & Oppenheim, C., "Legal Issues for Information Professionals, Part III: Data Protection and the media — Background to the Data Protection Act 1984 and the EC Draft Directive on Data Protection," *Journal of Information Science Principles & Practice,* Vol. 19, No. 2, 1993, pp. 85-97.

[13] Ellis, S. & Oppenheim, C., "Legal Issues for Information Professionals, Part IV: Attitudes to Data Protection Amongst UK Media Librarians," *Journal of Information Science Principles & Practice,* Vol. 19, No. 2, 1993, pp. 99-117.

[14] Gardner, E.P. et al. "The Importance of Ethical Standards and Computers Crime Laws for Data Security," *Journal of Information Systems Management,* Fall 1989, pp. 42-50.

[15] Gray, P.J., "Federal Privacy Legislation," *Credit World,* Vol. 78, No. 4, March/April 1990, pp. 18-22.

[16] Jones, M.R., "Protecting IT," *Director,* August 1993, pp. 47-52.

[17] Kallman, E.A & Grillo, J.P., *Ethical Decision Making and Information Technology: An Introduction with Cases,* Mitchell McGraw-Hill, 1993.

[18] The Law Reform Commission of Hong Kong, Privacy Sub-committee, *Reform of the Law Relating to Information Privacy : A Consultative Document,* May 1993.

[19] Lee, M.K.O., "Computer Crimes Legislation in Hong Kong — Recent Developments," *Datapro Reports on Information Security,* McGraw-Hill, April 1993.

[20] Longenecker, J.B., "Do Smaller Firms Have Higher Ethics?" *Business and Society Review,* No. 71, Fall 1989, pp. 19-21.

[21] Martinsons, M.G., "Cultivating the Strategic Use of Information Technology: Lessons from Hong Kong," *Technology Analysis & Strategic Management,* Vol. 3, No. 2, Summer 1993, pp. 179-186.

[22] Martinsons, M.G., "Global success with electronic banking: the Hong Kong Bank and Hexagon," *Journal of Strategic Information Systems,* Vol. 1, No. 5, pp. 290-296.

[23] McFarlan, F.W., "Information technology changes the way you compete," *Harvard Business Review,* Vol. 62, No. 3, May/June 1984, pp 98-103.

[24] McFarlan, F.W., "The 1990s: The Information Decade," *Business Quarterly,* Vol. 55, Iss. 1, Summer 1990, pp 73-79.

[25] Moulton, S., "The UK Data Protection Act 1984," *Journal of Information Science Principles & Practice,* Vol. 15, No. 1, 1989, pp. 55-56.

[26] Noble, P., "Fur Ex Machina," *Credit Management,* February 1990, pp. 19-22.

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

28] Oz, E., "Ethical Standards for Information Systems Pro-

fessionals: A Case for a Unified Code," *MIS Quarterly,* Vol. 16, No. 4, December 1992, pp. 423-433.

[29] Parker, D.B., Swope, S. & Baker, B.N., *Ethical Conflicts in Information and Computer Science, Technology, and Business,* QED Information Sciences, 1990.

[30] "Police Train for Crackdown: Computer Society, City Polytechnic team to provide computer crime courses," *Information Systems Management Newsweekly* (Hong Kong), Vol. X, No. 14, January 1993, p. 14.

[31] Regan, P.M., "The Globalization of privacy: Implications of recent changes in Europe," *American Journal of Economics & Sociology,* Vol. 52, No. 3, July 1993, pp. 257-274.

[32] Ritseman, H.A., "Information Technology and the Law," *International Journal of Technology Management,* Vol. 4, Nos. 4/5, 1989, pp. 551-562.

[33] Sizer, R. & Newman, P., *The Data Protection Act: A Practical Guide for Mangers and Professionals,* Gower, 1984.

[34] Straub, D.W. & Collins, R.W., "Key Information Liability Issues Facing Managers: Software Piracy, Proprietary Databases, and Individual Rights to Privacy," *MIS Quarterly,* Vol. 14, No. 2, June 1990, pp. 143-156.

[35] Tarrant, P., "Personal Data: The Act Begins to Bite," *Industrial Management & Data Systems,* Vol. 7, No. 1, 1990, pp. 11-14.

[36] Task Force for the Revision of the ACM Code of Ethics and Professional Conduct, "ACM Code of Ethics and Professional Conduct," *Communications of the ACM,* Vol. 35, No.5, May 1992, pp. 94-99.

[37] Towers, D.K., "The Privacy Challenge on Capitol Hill," *Marketing Research,* Vol. 3, No. 4, December 1991, pp. 60-62.

38] Tuerkheimer, F.M., "The Underpinnings of Privacy Protection," *Communications of the ACM,* Vol. 36, No. 8, August 1993, pp. 69-72.

[39] Wong, E.Y.W., "Issues related to data protection legislation in Hong Kong," *Proceedings of the Singapore ICCS/ISITA '92 Conference,* November 1992, pp. 253-256.