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 center 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].

Computer pose a potential danger to individual privacy [26,11,32,33]. 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 considerations of ethical and privacy matter [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 computer and telecommunications techniques [1,15,25,37,38]. The recent explosions of IT use in Hong Kong (and more generally Asia) combined with the lack of legislation to project 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 computerized personal data are not directly liable for a criminal offence. This situation is a significant business and social concern in Hong Kong [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. TDF's 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 issues in 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 data protection 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 Transfer 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 prompt the establishment of the Privacy Sub-committee to study data protection-
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. The following are likely constraints on the territory’s international trade, rising information management controversy and declining public confidence in the information trade industry.

The Hong Kong proposals are in line with international agreements. They place a high emphasis on data protection practices. Many Western countries already have data protection legislation in place. In particular, the Data Protection Act of 1984 [9] deals with data protection matters. Many business activities 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 misdescribing 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

Journal of Information Technology Management, Volume V, Number 3, 1994 61
CONCLUSIONS

The Hong Kong Government has recognized the importance of having data protection law in the territory [10,19]. However, implementation and enforcement will not be simple matters. Other countries have experienced an assortment of implementation enforcement problems [12,13,38]. The regulation system of the United Kingdom’s Data Protection Act has been criticized as being too complex and cumbersome. Some major small businesses 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 practiced around the world. Its aim 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 [10,11]. The legislative 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 property, 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, an increasing number 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 most novel to most individuals and organizations in Hong Kong and the region [10,21]. New legislation in this area will transform, or at least alter, many business management practices [8,20]. Senior 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 personal data [35]. Individuals will have to be made aware that misuse of personal data, no matter how trivial, is an infringement of privacy.
REFERENCES

[12] Ellis, S. & Oppenheim, C., "Legal Issues for Information Professionals, Part III: Data Protection and the me-

[28] Os, E., "Ethical Standards for Information Systems Pro.
Conflicts in Information and Computer Science, Technology,
and Business, QED Information Sciences, 1990.
[34] Straub, D.W. & Collins, R.W., "Key Information Li-
ability Issues Facing Managers: Software Piracy, Pro-
[38] Twerskheimer, F.M., "The Underpinnings of Privacy Pro-
[39] Wong, E.Y.W., "Issues related to data protection legis-
lation in Hong Kong," Proceedings of the Singapore
ICCS/ISITA '92 Conference, November 1992, pp. 233-
256.