1. What is Privacy?

In his comprehensive review of the question, Professor Raymond Wacks of the University of Hong Kong concludes that "in spite of the huge literature on the subject, a satisfactory definition of "privacy’ remains as elusive as ever”. Similarly, the United Kingdom committee on Privacy ("The Younger Committee") concluded in its 1972 report that the concept of privacy could not be satisfactorily defined. Instead, it sought to identify the values in which privacy was a major element and determine which of those values deserved protection.

This approach was also taken by the Australian Law Reform Commission in its 1983 report on privacy. The "interests” which it identified with the concept of privacy were:

1. the interest of the person in controlling the information held by others about him, or "information privacy” (or "informational self-determination” as it is referred to in Europe);
2. the interest in controlling entry to the "personal place”, or "territorial privacy”;
3. the interest in freedom from interference with one's person, or "personal privacy”;
4. the interest in freedom from surveillance and from interception of one communications, or "communications and surveillance privacy”.

2. Privacy and Personal Data Protection

Personal records have been with us as long as the written word, but the advent of the computer about 50 years ago and the subsequent rapid advances in computer technology pose practical implications for privacy as identified by a 1975 UK white paper:
1. they facilitate the maintenance of extensive record systems and the retention of data in those systems;
2. they can make the data easily and quickly accessible from many different points;
3. they make it possible for data to be transferred quickly from the information system to another;
4. they make it possible for data to be combined in ways which might not otherwise be practicable; and
5. because the data are stored, processed and often transmitted in a form which is not directly intelligible, few people may know what is in the record or what is happening to it.

It is therefore not surprising that opinion polls in industrialised countries have revealed a growing concern for individual privacy that clearly transcends national boundaries.

Countries with the earliest data protection laws include Sweden (1973), USA (1974), Germany (1977), Austria (1978) and Denmark (1978). To date around 40 jurisdictions have enacted laws to protect privacy with respect to personal data. The majority is European. However, in the immediate region, Taiwan has recently passed such a law and Japan has had one since 1988. Elsewhere in the Pacific Rim, Australia, New Zealand and Canada all have such laws.

Apart from the protection of privacy, another impetus towards the proliferation of legislative measures is the issue of transborder data flow.

3. Transborder Data Flow (TDF)

The increasing use of computers has coincided with a communications boom resulting in a massive increase in international telecommunications traffic. The transborder data flow of personal data is generated, where, for example, flight reservations are made in another country or foreign tourists use credit cards, or securities of a foreign market are bought. While a passenger will not oppose to the transfer of data to another country to facilitate the flight, privacy issues arise if the data are used for other purposes, such as marketing of other products to the passenger.

In a comprehensive review of the issue, an academic has pointed out that "the extended possibilities to transmit information almost without reference to distance, time
or volume has given rise to a spectacular growth in data flow through the use of the international telecommunication networks”. This data traffic has been aptly described as "the life-blood of modern business life”. As the Hong Kong Law Reform Commission report pointed out, the dilemma arising from this ever increasing flow of personal data between countries derives from their greatly variable levels of privacy protection.

Those countries that have already established data protection laws are concerned that privacy protection is being undermined by the unrestricted transfer of personal data to other jurisdictions which lack the internationally accepted for the processing and storage of personal data. A large number of industrialised countries now possess data protection laws, and increasingly these laws restrict the transfer of data to countries lacking adequate data protection.

It was this threat of interference that led to the Organisation for Economic Co-operation and Development (OECD) issuing in September, 1980, its Guidelines on the Protection of Privacy and Transborder Flow of Personal Data, which include a set of personal data protection principles. It should be noted that from October, 1998 all European Union member states are required to have in place data protection measures that, among other things, satisfactorily deal with the transborder data flow issues, as required by the 1995 Union Directive on the protection of Personal Data. The Directive also expects third countries should have adequate measures to protect personal data given the increasing data traffic between the European Union and other countries.

4. Hong Kong Scenario

In Hong Kong, concern over the threat to privacy posed by technological developments can also be traced back to the 1970's. As elsewhere, commentators were not slow to recognise the privacy threats posed by such developments and the possibility that the free flow of personal data to places without adequate privacy protection would be impeded. The Government's initial response was the promulgation in 1988 of the Data Protection Principles and Guidelines, which are based on the OECD guidelines I have referred to. Voluntary compliance was invited to these guidelines from the private and public sectors. The Government also accepted in principle that data protection legislation
should be enacted in Hong Kong.

The main work on developing a legislative model for Hong Kong was undertaken by the Law Reform Commission (LRC), which began to do this in 1990. In 1993 the LRC’s Privacy Sub-committee conducted a thorough public consultation exercise based on a lengthy document containing detailed initial proposals. Over 100 substantive responses were received by the Sub-committee, which also participated in a series of seminars on its proposals. The end result of this work was the LRC’s report on reform of the law relating to the protection of personal data published in August 1994.

Based on the LRC’s recommendations, the Personal Data (Privacy) Bill was introduced into the Legislative Council in April 1995. It was examined by a Bills Committee with further public consultation. Subsequent to the deliberations of the Bills Committee, the Bill was subject to lengthy debate in the full Legislative Council and the Ordinance was signed into law on 3 August 1995.

5. The Personal Data (Privacy) Ordinance

The purpose of the Ordinance is to protect the privacy interests of living individuals in relation to personal data. It also contributes to Hong Kong’s continued economic well being by safeguarding the free flow of personal data to Hong Kong from restrictions by countries that already have data protection laws.

For those who are familiar with the topic of personal data protection, you will find that our Ordinance is quite a progressive law, in that:

1. it covers both automatic and manual data;
2. it covers both the public and private sectors; and
3. it establishes an independent statutory body which has wide-ranging investigation and enforcement powers to be exercised when and where appropriate to ensure compliance.

6. Personal Data

“Data” is defined in the Ordinance as any representation of information (including an expression of opinion) in any document, and includes a personal identifier, and
"Personal Data" is defined as any data -

1. relating directly or indirectly to a living individual;
2. from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
3. in a form in which access to or processing of the data is practicable.

7. Data Protection Principles

Six personal data protection principles, which are in line with international practice and are based on the OECD guidelines, are enshrined in the Ordinance:

1. Principle 1 - Purpose and manner of collection - this provides for the lawful and fair collection of personal data and sets out the information a data user must give to a data subject when collecting personal data from that subject.
2. Principle 2 - Accuracy and duration of retention - this provides that personal data should be accurate, up-to-date and kept no longer than necessary.
3. Principle 3 - Use of personal data - this provides that unless the data subject gives consent otherwise personal data should be used for the purposes for which they were collected or a directly related purpose.
4. Principle 4 - Security of personal data - this requires appropriate security measures to be applied to personal data.
5. Principle 5 - Information to be generally available - this provides for openness by data users about the kinds of personal data they hold and the main purposes for which personal data are used.
6. Principle 6 - Access to personal data - this provides for data subjects to have rights of access to and correction of their personal data.

8. Exemptions

The Ordinance provides specific exemptions from the requirements of the Ordinance. They include:

1. a broad exemption from the provisions of the Ordinance for personal data held for domestic or recreational purposes;
2. exemptions from the requirements on subject access for certain employment-related personal data; and
3. exemptions from the subject access and use limitation requirements of the Ordinance where their application is likely to prejudice certain competing public or social interests, such as: security, defence and international relations; prevention or detection of crime; assessment or collection of any tax or duty; news activities; and health.
9. Functions and Powers of the Privacy Commissioner for Personal Data:

The main functions and powers of the Privacy Commissioner are to:

1. monitor and supervise compliance with the provisions of the Ordinance;
2. approve and issue codes of practice giving practical guidance for compliance; with the provisions of the Ordinance;
3. specify classes of data users required to provide information concerning their personal data practices for compilation of a public register of data users;
4. approve the automated matching of personal data;
5. promote awareness and understanding of, and compliance with, the provisions of the Ordinance;
6. carry out inspections of personal data systems, including those of Government departments and statutory corporations; and
7. investigate, upon receipt of complaints from data subjects or on his own initiative, suspected breaches of requirements of the Ordinance.

10. Codes of Practice

The Commissioner is vested with the power to issue and approve codes of practice for data users for the purpose of providing practical guidance in respect of requirements under the Ordinance. Since 1997, three Codes of Practice have been issued after extensive public consultation.

2. Code of Practice on Consumer Credit Data 1998

In late 2000, announcement was made to publish a Code of Practice for Workplace Surveillance. This Code will deal with the more common forms of workplace surveillance, including e-mail, telephone and CCTV. It is planned for a draft document to be published in 2001 for extensive public consultation.
11. Enquiries, Complaints & Investigations

11.1. Enquiries received during 1999-00

11.1.1. Figure 1 - Annual enquiry caseload

In the reporting period, the PCO handled a total of 15,557 enquiry cases. On average, some 57 cases were received per working day.

![Figure 1](image)

11.1.2. Figure 2 - Nature of enquiry cases

Of the 15,557 enquiry cases handled in the period under review, approximately 63% of the cases (9,798) were queries related to privacy rights specific to an individual’s own situation. A further 22% of the cases (3,416) were queries related to the application of the requirements of the PD(P)O. Another 10% of the cases related to queries and requests about publications issued by the PCO. The remaining 5% involved queries concerning the functions of the PCO.
11.1.3. Figure 3 - Means by which enquiries were made

In the reporting year, the PCO handled 13,951 calls on the enquiry hotline (telephone number 2827 2827). Of these, 99% of them received an immediate response or a callback by our enquiry officers within 2 days.

Written enquiries are received by the PCO in the forms of letters, faxes or emails. In the reporting year, a total of 1,302 written enquiries were handled. Of these, 87% of them received a substantive reply within 28 days.
11.2. Complaints received during 1999-00

11.2.1. Figure 4 - Annual complaint caseload

In the reporting year, the PCO received 568 new complaints of possible breaches of the PD(P)O. Compared with the 418 complaints received in 1998-99, this represented a 36% year on year increase in the complaint caseload.

![Figure 4](image)

11.2.2. Figure 5 - Types of party complained against

Of the 568 complaints received in the reporting period, 70% (398) of the cases were complaints against private sector organizations. Compared with the 287 cases received in 1998-99, this represents a 39% increase in this category of complaints.

A further 17% (97) of the cases were complaints lodged against a third party individual. This was more than double the 47 cases received in 1998-99. This indicates a growing trend in which personal grievances between individuals are being brought to the attention of the PCO.
12. Date Privacy and Electronic Commerce

It is Government policy to establish Hong Kong as an information society and a global player in electronic commerce. Apart from building our physical and business infrastructure, ensuring the trust and confidence of our consumers would enhance our ability to meet this goal. Complementing the regulatory requirements of the PD(P)O, our office is working with many professional and industry bodies, as well as relevant government and statutory bodies to implement self-regulatory initiatives pertinent to the protection of data privacy. For example, our office has been working closely with the Hong Kong Society of Accountants with its launch of the WEBTRUST seal in 2000 for local websites, the display of which at a website provides assurance to consumers of its compliance with a set of auditable principles and procedures which protect consumers' interests including data privacy. Another relevant example is our joint work with the Hong Kong Internet Service Providers Association (HKISPA) and the Office of the Telecommunications Authority (OFTA) on the development of a Spamming Code of Practice for compliance by the ISPs in Hong Kong to reduce the amount of spamming activities which are regarded by many as nuisance and privacy intrusive. Through the active promotion of the requirements of the data protection principles and the Ordinance for incorporation into the implementation plans for our electronic businesses and services,
our consumers can embrace the New Economy with confidence and trust.

13. Conclusion

Increasingly aware of the importance of privacy to our community and assisted by our Office's education and publicity campaign on the requirements of the PD(P)O, organizations in Hong Kong realize the positive impact of compliance with the Ordinance in the collection and use of personal data of their customers and employees. Our Annual Opinion Surveys over the last four years have found that organizations which agree that compliance with the PD(P)O would bring about long term benefits to the organization have increased substantially over the years. The benefits are accrued in the areas of customer relationship, employment relationship, public image and corporate management. For example, 86% of the organizations surveyed in 2000, as compared to only 59% in 1997, agreed that compliance with the Ordinance would bring about long-term benefits to the public image of the organizations.