Speech for the Hong Kong International Computer Conference
26 September 2008

"Impact of Technology on Data Privacy"

Good afternoon, ladies and gentlemen,

At the outset, I must declare that I am far from being an IT expert and I can't pretend to share with you here any specific IT knowledge. However, as fellow travelers on this technological super highway, we need to mind where we are heading because any wrong turn may lead us down some slippery path. While enjoying the positive benefits of staying globally connected through the use of internet and email and other electronic devices, we are constantly alarmed by the number of incidents involving data losses and leakages. Mishaps still fresh in the public memory include the Independent Police Complaints Council incident concerning leakage on the internet of personal data of those citizens who had made formal complaints against individual police officers; the online dissemination of nude photos of well-known actresses and the recent spate of losses of patients' data by the Hospital Authority. These incidents have given me sleepless nights not to mention weeks' and months' work. The gravity of the situation depends on the number of individuals affected, the sensitive nature of the personal data involved and the difficulty in curbing further spread of the data leaked or lost in each case. The damage caused to the data subjects can be far-reaching but not easy to quantify. I am therefore glad to have the opportunity here to share with you my experience as a privacy regulator on the practical steps in taking to protect personal data privacy in facing up to the challenges posed by technological advancements.

Hong Kong can be proud to have the only independent privacy commissioner in Asia. After New Zealand's Privacy Act 1993, our Personal Data (Privacy) Ordinance (enacted 12 years ago) was the second privacy law outside Europe to cover both the private and the public sectors. Our privacy legislation is technology-neutral, which means that whatever the media or devices used by a data user to collect and handle personal data, the requirements of the Ordinance, in particular, the six data protection principles have to be complied with. The six data protection principles embody a data processing cycle from collection, retention, use, security to the right of data

subjects to access and correct personal data about them held by the data users. These six principles are the cornerstone of international data protection standards. Under our law, the breach of a data protection principle *per se* does not attract criminal sanction, but upon a finding of contravention of any such principle following an investigation, I may serve an enforcement notice directing the data user to take specific remedial steps. The failure to comply with the enforcement notice is an offence punishable under the Ordinance. I will focus today mainly on two issues. One is the collection of biometric data and the other is the measures to be taken when a breach of data security occurs.

Collection of fingerprint data

During the past three years of my term of office, I have witnessed an increasing trend of the use of fingerprint scanners to collect personal data. A typical example is when employers collect their staff's fingerprints and use them for recording attendance at work. The employers believe this method is more effective than the use of electronic access cards in preventing "buddy swiping". I have also encountered cases where fingerprint scanners were used by a primary school to record the use of facilities, such as library and canteen by students who were not older than 12. Fingerprints are regarded as particularly sensitive personal data because they are unique and permanent, but the risk of identity theft associated with fingerprints are very real.

In order to facilitate compliance with the collection limitation principle that only necessary, adequate but not excessive personal data are to be collected by the data user, I had issued a guidance note on "Collection of Fingerprint Data" in August last year. In assessing whether the collection of fingerprint data is necessary to attain the purpose of collection, it is important that the data user should take into account the degree of intrusion into personal data privacy brought by such a practice on the one hand and the appropriate measures to be taken to mitigate the adverse privacy impact on the other. The stance my Office has adopted on the collection and use of fingerprints is that a data user should, as far as practicable, obtain the "informed consent" from the data subject.

To ensure that "informed consent" is obtained, I consider it essential that two requirements should be met. First, the data subject does possess the

capacity to understand the adverse impact on his personal data privacy; and secondly, that there be no undue influence exerted upon the data subject when his consent is sought. To illustrate the first requirement, a data user should avoid collecting fingerprint data from children of tender age or persons who suffer from mental incapacity. Thus, in the example I just quoted of the primary school which used fingerprint scanners for recording attendances as well as the use of library and canteen facilities by its students, I was not satisfied that there was an "informed consent" even though the school claimed that consent had been obtained. If children are exposed too early in life to an environment where sensitive personal data are easily demanded and given, they may grow up with a lower level of privacy awareness. In relation to the second requirement, in the case where there is an employer-employee relationship unavoidably there is a presumption that a disparity of bargaining power exists. The fact that an employer has genuinely offered its employees alternative choices if the employees do not wish to surrender their fingerprint data will be viewed favorably by me as supporting evidence that any consent obtained from the employees is freely given.

Security breach and containment measures

Next, I shall talk about the topical issue of data security breach. Our law requires that a data user shall take all reasonable practicable steps to protect personal data against unauthorized or accidental access, processing and use. Although this requirement does not impose an absolute duty upon a data user to guarantee data security, the level of security measures to be taken by a data user should be appropriate to the sensitivity of the personal data concerned and the degree of harm that would follow in the event of data security breach. I shall highlight two situations : one is where electronic personal data are collected and stored via portable electronic devices and the second is where these data are passed to third parties for handling or processing on behalf of the data user, e.g. by an IT contractor.

My Office recently carried out an inspection of the patients' data system maintained by the Hospital Authority which manages the majority of the hospitals in Hong Kong. At the end of the Inspection, I offered no less than 37 recommendations to the Hospital Authority which accepted them and promised that they will be implemented. One of my recommendations is that

the Hospital Authority should minimize the use of HKID number of the data subjects. As in too many cases, a great number of the data leakage incidents are caused by human error. One of the recommendations I made was that the personal data should be de-identified as far as practicable, e.g. the use of code that is identifiable only within the data user's system, for example, hospitals' patient numbers. More stringent measures to control and regulate the downloading of identifiable personal data through the use of industry standard encryption especially when USB flash drives or other portable devices are used. The importance of secure erasure of personal data which are no longer required is also highlighted in my Inspection Report.

When data users transfer personal data to contractors for processing, they should take steps to comply with the law and insofar as is possible not to give the contractor live personal data to work off-site.

Prevention is always better than cure is an axiom that also applies to the protection of personal data. Hence, where a new project or undertaking is to be launched involving the collection and holding via electronic means of a large number of personal data or personal data of a sensitive nature, the data user is advised to undertake a privacy impact assessment. Due consideration should be given to the implementation of appropriate security measures and privacy enhancement technologies. PIA as we call it should be a standard procedure to be followed by organizational data users. One live example in Hong Kong is when the Immigration Department introduced the SMART ID cards in June 2003. The Immigration Department realized the need to protect the sensitive personal data in the "chip" embedded in the card and that proper handling of the large database involves careful risk management. They therefore undertook no less than 4 PIAs before actually going ahead with the project.

In the unhappy event of a security breach, a data user should take prompt steps to contain the breach and to repair any systemic loopholes as soon as possible so as to contain the breach and to mitigate any damage. If the breach is likely to cause a real risk of serious harm to the data subjects, the data user ought to consider giving a data breach notification so that remedial actions can be taken. Although the Ordinance does not require a breach notification, it has been the consensus of the international data protection authorities to recommend data users to seriously consider in the particular circumstances of

the case whether it is a good containment measure to take.

The legislative reform

In order to ensure that our privacy legislation keep pace with modern changes, my Office has made a comprehensive proposal and suggested more than 50 amendments to the Ordinance. Some of these amendments deal with issues such as whether data processor's act or conduct be regulated under our law, whether an offence should be created to deal with the reckless and wanton behavior of persons who obtained personal data without the consent of the data users and whether a higher level of personal data protection be afforded to data which are rightly regarded as sensitive.

Personal data privacy is not an absolute right and a proper balance must be struck with other competing rights and public interest. I hope the Government will give full consideration to my proposal and to solicit public responses through consultation. To end my speech, I appeal to you for your support in building a sound and healthy world where technology and privacy live and thrive together comfortably. Thank you.

Roderick B. Woo
Privacy Commissioner for Personal Data, Hog Kong

--- END ---