個人資料私隱專員公署的信頭

Letterhead of Office of the Privacy Commissioner for Personal Data

(By Hand)

Our Ref: PCO/8/2
Your Ref: CB1/BC/19/98

16 November 1999

Clerk to Bills Committee
Legislative Council
Legislative Council Building
8 Jackson Road
Central
Hong Kong

Attn: Miss Salumi CHAN

Dear Miss Chan,

Bills Committee on Electronic Transactions Bill

Thank you for your letter (wrongly dated 15 November 1999) which we received on 8 November 1999 and the attached paper on "Digital certificates and privacy" forwarded by the Hon SIN Chung-kai, Chairman of the Bills Committee.

Our Office have previously been consulted by the Information Technology and Broadcasting Bureau on the draft Electronic Transactions Bill. In response, we have already forwarded our comments on the draft to the ITBB. In this respect, we have no further comments to offer on the Bill.

Nevertheless, we have prepared a paper on the issue of "Data Privacy and Digital Certificates", a copy of which is enclosed with this letter. You may wish to forward it to the Chairman for his reference.

Yours sincerely,

(Tony LAM)
Acting Privacy Commissioner for Personal Data

Encl.

Data Privacy and Digital Certificates

Electronic commerce, conducting business over Cyberspace, is growing at a phenomenal rate. In Hong Kong, there are already commercial organisations that offer business transactions online over the Internet, for example, the "Citidirect" online banking facilities of Citibank and the "Shopping baskets" online purchase facilities of the Chinese Books Cyberstore. In addition, the Hong Kong Government has decided to launch its "Electronic Service Delivery" scheme sometime in late 2000 that will make available public services online, 24 hours a day, seven days a week. The indications are that more and more local companies will offer electronic services in line with global trend.

2. As more and more commerce and government services are delivered electronically over Cyberspace, vast quantities of personal data about all of us will potentially be collected, stored and transmitted through Cyberspace. The past's great protectors of privacy: cost, distance, incompatibility, etc., are all disappearing in this Cyberspace.

3. The major issue of concerns in electronic commerce is to do with ensuring trust and confidence of both the consumers and the businesses. Of all these concerns related to trust and confidence, data privacy is regarded as dominant.

Data Privacy Concerns

4. In electronic commerce, concerns over privacy emerge when an individual is requested to provide personal data, for example, name, address, credit card number, etc., as part of an online transaction when he or she is dealing with a business partner over an open and unmanaged network such as the Internet. These concerns are two folded.

a) **Security threat.** This relates to the protection of personal data transmitted over the Internet. Unless security measures are taken, there exist the dangers of data being intercepted during transmissions as well as the risks of data being modified, often without the knowledge of the individuals concerned.

b) **Privacy intrusion.** This is to do with the unfair and unlawful collection of personal data by misrepresentation of identities of trading partners as well as their use for fraudulent or unintended purposes for

which the individuals concerned have not consented to. Indeed, not only are our personal data transmitted over the Internet accessible to others, marketers can systematically data mine the Net to assemble personal profiles and target lists for market research and direct marketing.

Protecting Data Privacy

5. In Hong Kong, personal data privacy is protected by the Personal Data (Privacy) Ordinance. The objective of the Ordinance is obviously to protect the privacy interests of living individuals in relation to personal data. It also serves a less well-known, but a definitely not less important purpose in contributing to Hong Kong's continued economic well being by safeguarding the free flow of personal data to Hong Kong from restriction by countries that already have data protection laws.

6. Local organisations are within Hong Kong's jurisdiction. The basic legal principle is *"What is illegal offline must also be illegal online"*. Therefore, frauds in Cyberspace, for example, using stolen credit card number to do online purchase, or setting up a Web site to defraud the public, will be prosecuted under our criminal laws.

Electronic Transaction Bill

7. To provide the necessary legislative support for the conduct of electronic transactions in Hong Kong, the Government introduces the Electronic Transaction Bill to give legal recognition to electronic records and digital signatures. The Bill also provides for the Hongkong Post to commence certification service operations to issue and manage electronic certificates ("e-Cert") to legal entities in Hong Kong so as to authenticate the identity of participants in electronic commerce.

8. According to the Hongkong Post, each e-Cert user will have a pair of keys - a private key and a public key. The private key is kept secret, known only to the holder; the other key is made public by placing it in a public key directory. When a sender electronically signed a message with his or her private key, the recipient can validate the signature only with the sender's public key that is open to the public. The HongKong Post manages and distributes public keys and digital certificates through the establishment of a key management infrastructure called the Public Key Infrastructure ("PKI").

Potential Privacy Threats

9. It is widely believed that development and use of certification authorities ("CA") and key encryption technology will be essential for secure and trusted electronic transactions, and consequently, will become a prerequisite to participation in electronic commerce. The public key cryptography addresses issues of data integrity and transaction privacy whereas electronic certificates address concerns of authentication and access control.

10. Whilst the technology associated with the PKI indicates positive effort towards data security, there are potential threats to data privacy ancillary to their employment. The following are some aspects of concern.

a) **Public key directory.** The most important function of a CA is to certify the pubic keys used in digital certificates. A digital certificate will hold identity data about the holder, e.g. name or identity card number for key certification purpose. A digital certificate may also hold demographic data about the holder, e.g. sex or date of birth that can be used to allow the holder to gain access to customised contents of certain web sites that accept digital signatures in lieu of a password. However, digital certificates are automatically listed in the CA's public directory and their contents can be viewed by anyone who looks them up from the directory. Unless protection measures are applied to the more sensitive data such as the individual's identity card number, this open access of the certificates may give rise to the unnecessary exposure of personal data that may subsequently be mis-used for other unintended purposes.

b) **Key recovery.** Cryptographic techniques make possible information data secure from unwanted interception, eavesdropping and theft by third parties. However, strong encryption has an ancillary effect. It becomes more difficult for law enforcement agencies to gain access to encrypted information records of suspected criminals without the knowledge and assistance of the target. This difficulty has arguably led to a government-access requirement that attempts to associate key recovery with key certification. The requirement creates the existence of a "back-door" secret key that is maintained to make decryption information quickly accessible to law enforcement agencies without notice to the key owners. Unless specific safeguards are built to restrict access to and justify the use of such recovery capability, this third party lawful access would create additional privacy risks.

c) **Identity tracking.** In a report recently released by cryptographic researchers in Holland, the authors remarked that if measures are not taken to enhance the integrity of digital certificates, there is the prospect that "*everyone [will be] forced to communicate and transact in what will be the most pervasive electronic surveillance tool ever built*". The sort of concerns stems from the fact that every digital certificate will be capable of being traced uniquely to the person to whom it has been issued, or to the device in which it has been incorporated. These certificates could then be tracked as they move through the system, thereby enabling files of personal transaction data to be compiled, linked or cross-tabulated with third party information and used for profiling purposes.

Conclusion

11. The application of cryptographic techniques in an electronic transactions environment can address issues of security protection: to guarantee that contents of a transaction have not been altered (integrity), to establish the identity of the parties to the transaction (authentication), or to make legal commitments (non-repudiation). However, it is not adequate, by applying cryptographic techniques in isolation, to address the issue of privacy protection in relation to unfair collection of personal data or unauthorised use of the data for purposes for which the individuals concerned have not consented to. Efforts taken to effectively promote the integrity of the electronic transaction business should address both the security and privacy needs simultaneously.

12. As part of any certification service operations, it is therefore important that sufficient care should be taken to protect users' data privacy by implementing practicable privacy enhancing measures that are developed based on well established privacy protection policies and guidelines. These policies should include matters such as the limitation on the personal data collected necessary for the provision of the service, the amount of information to be published about issued certificates that would fulfil the purpose of confirming their validity and the rules relating to disclosing certificate data to third parties for purposes other than those for which they were collected.

Office of the Privacy Commissioner for Personal Data
November 1999