Our Ref. : PCO/8/2/ pt.9
Your Ref. : CBI/BC/16/02

19 March 2004

Miss Polly YEUNG
Clerk to the Bills Committee
Legislative Council
Legislative Council Building
8 Jackson Road, Central
Hong Kong

By Hand

Dear Miss YEUNG,

Electronic Transactions (Amendment) Bill 2003 ("the Bill")

I refer to the letter dated 27 February 2004 inviting submissions on the Bill. Having perused the amendments proposed for the Electronic Transactions Ordinance, Cap. 553 ("ETO"), I have the following observations to make.

I. Personal data that are made publicly available

The disclosure record ("disclosure record") for the certification authority

Under the proposed new Section 43A(3), the Director of Information Technology Services ("the Director") must publish in the disclosure record ('the disclosure record") for the certification authority, *inter alia*, the material information in any of the assessment report and statutory declaration when the Director considers that major changes are occurring. Section 31 of the ETO requires the Director to maintain the disclosure record which is an on-line and publicly accessible record and that the information relevant for the purposes of the ETO must be published. This has the effect akin to a public register. From the wording of the proposed amendments, it appears that what information is regarded as material is entirely a matter for the Director to decide.

The disclosure record that we have seen does not appear to contain personal data. However, if disclosure record were, for whatever reason, to contain personal data, then the requirements under the Personal Data (Privacy) Ordinance ("the PDPO"), in particular, the protection against use for unrelated purposes in breach of data protection

principle ("DPP") 3 shall be properly addressed. The provision of a purpose statement specifying the use of the personal data in the proposed amendments will then be important and effective in quelling any uncertainty over the permitted use. Although a purpose statement may be given by means other than through legislative enactment, the clarity and force of statute is authentic guidance to a data user. Perhaps members of the Bills committee may consider it relevant and timely to include a clear purpose statement for permitted use in the Bill.

In maintaining a public register, the Director's attention is also drawn to the recommendations made by the Home Affairs Bureau in its memo captioned "Review of Public Registers" issued on 30 December 2000 (ref: (47) in HAB/II/6/32 III) for implementation of appropriate administrative measures to facilitate compliance with the PDPO.

The repository

Amendments proposed for section 36 concern the provision for publication in a repository by the certification authority of recognized certificates issued by it and accepted by the person named or identified therein. According to the definition laid down in section 2(1) of the ETO, a repository will store information relevant to the certificates and are retrievable. Given that a recognized certification authority is required under Section 45 of the ETO to maintain an on-line and publicly accessible repository containing personal data belonging to holders of the certificates, a purpose statement specifically defining the purpose of use is helpful in guarding against misuse of the personal data.

The inclusion of a purpose statement in the Bill defining the purpose(s) of keeping the repository and the permitted use of personal data obtained is therefore recommended for the Bills Committee's consideration.

II. The collection of personal data by the Director and the certification authorities

It is noted that the Director is vested with powers under section 30 of the ETO to specify any particulars and documents to be furnished by the certification authorities. Powers are also conferred under section 33 for the Director to issue code of practice specifying the standards and procedures for carrying out the functions of recognized certification authorities. Insofar as collection of personal data is concerned, the Director and the recognized certification authorities as data users shall ensure compliance with the requirements of the PDPO in particular DPP1 that personal data collected shall be adequate but not excessive for the purpose of collection. All practicable steps shall also be taken by the Director and the recognized certification authorities respectively on or before the collection of personal data to notify the data subjects of the purpose of

collection and the classes of persons to whom the personal data may be transferred. The giving of written Personal Data Collection Statement to the data subjects is therefore a recommended good practice to follow.

I am pleased to submit the above for your kind consideration.

Yours sincerely,

(Raymond TANG)
Privacy Commissioner for Personal Data

Encl. : a soft copy of the English and Chinese versions of this letter

c.c. The Secretary for Commerce, Industry and Technology
(Attn.: Miss Adeline WONG / Mr. Howard LEE, File Ref: ITBB/IT 107/4/8(02) Pt II)