Our Ref: PCO/CR/6/23
Your Ref: CB2/BC6/01

23 October 2002 (by fax & email)

Mrs Sharon Tong,
Clerk to Bills Committee,
Legislative Council,
3/F., Citibank Tower,
3 Garden Road,
Central, Hong Kong

Dear Mrs Tong,

Bills Committee on
Registration of Persons (Amendment) Bill 2001

Thank you for your letter dated October 17, 2002.

By the time your letter reached us, we have already prepared a paper on privacy audit, which was requested by the Hon IP Kwok-him, Bills Committee Chairman, towards the conclusion of the meeting on 11th October. I have pleasure in enclosing herewith the subject paper (in Chinese and English) and shall be grateful if you will kindly place the same before the Chairman.

The three items enumerated in your letter under reply encompass a much wider ambit. On the basis of our present understanding of the smart card regime, it is not possible for us to prepare a paper of substance that is meaningful and adequately addresses all three items. The Administration will need to come to a firm view on the structure and contents of a code of practice (item (a)) that would govern the entire operational framework (including all components within that framework) as between the departmental 'data users', and, if appropriate, factoring in 'outside (non-governmental) users' as well. When that stage is reached, the PCO will be pleased to offer its views and comments on any proposed code of practice, and, as mentioned in our paper, such code may be made the subject of approval pursuant to section 12 of the Personal Data (Privacy) Ordinance, thus giving the code statutory backing.

Our paper, as drafted, addresses specifically on the subject of privacy compliance audit and (in part) deals with certain elements of items (b) and (c). I trust that the Chairman and Members of the Bills Committee will find the contents helpful in their further deliberations.

Grateful if you will kindly convey my observations to the Chairman.

Yours sincerely,

Raymond Tang
Privacy Commissioner for Personal Data

Encl.

U:/kitty/kcmisc2.doc

PAPER FOR THE BILLS COMMITTEE
OF THE LEGISLATIVE COUNCIL
REGISTRATION OF PERSONS (AMENDMENT) BILL 2001

Privacy Compliance Audit: Smart Identity Card Scheme

INTRODUCTION

As requested by Members at the meeting on 11 October 2002, this paper provides information on the views of the Privacy Commissioner's Office ("the PCO") on the conduct of privacy compliance audit in relation to the smart Identity Card scheme of the Immigration Department.

WHAT IS A PRIVACY COMPLIANCE AUDIT?

2. A privacy compliance audit ("PCA") in relation to a personal data system is a systematic verification of compliance with privacy policies, data protection principles, codes of practice or other regulatory requirements with respect to information handling and privacy. The PCA examines the information management processes of the data system, assesses the extent to which the processes are implemented in accordance with stated privacy protection requirements, and provides assurance on the level of privacy compliance.

3. A privacy compliance audit is different from a privacy impact assessment ("PIA"). The latter is a process for evaluating a data system or policy proposal in terms of its impact upon privacy and determines how any detrimental effects upon privacy might be overcome in its implementation. In other words, a PIA is a pre-implementation event that needs to commence at the outset of any data system or policy proposal implementation. In contrast, a PCA is a post-implementation event. It verifies that all privacy issues identified in a PIA are properly addressed in the delivery of the data system, that safeguards to enhance privacy protection are implemented as promised and that control mechanisms are put in place to ensure on-going privacy compliance.

THE ROLE OF THE PRIVACY COMMISSIONER

4. Section 36 of the Personal Data (Privacy) Ordinance ("the PD(P)O") empowers the Privacy Commissioner to carry out inspections of personal data systems used by data users. The purpose of an inspection is to make recommendations to promote compliance with the requirements of the PD(P)O, in particular the data protection principles, by the data user inspected and, where appropriate, the class of users of which such data user is a member. Section 48 of the PD(P)O also provides for the Privacy Commissioner to publish a report setting out any recommendations to a class of data users arising from an inspection or investigation and in such manner as he thinks fit.

5. Since the commencement of the PD(P)O on 20 December 1996, the PCO had not been successful in securing the necessary resources for the inspection function. So far no inspections of personal data systems were carried out. Despite the non-provision of manpower resources, the PCO have been adopting a less formal approach in promoting privacy compliance. A "compliance check" is undertaken when the PCO identifies a practice of an organization that appears to be inconsistent with the requirements of the Ordinance. In such circumstances, the PCO invite the organization concerned to take immediate action to remedy the apparent inconsistency. It is also the policy of the PCO to encourage organizations to undertake self-monitored compliance assessments of their personal data management practices. To assist organizations in this respect, the PCO produced in 1999 a CD-ROM based privacy compliance self-assessment tool-kit (Privacy.SAFE) that helps data users to perform compliance checking.

6. In other jurisdictions where there are established privacy protection laws, the conduct of inspection or privacy compliance audit of data systems/practices is normally a function of the privacy or information commissioner. For example, the Australian Federal Privacy Commissioner has powers under the Privacy Act 1988 to audit government agencies' compliance with the Information Privacy Principles and to examine records in relation to "tax file number" information. The Privacy Act 1988 also empowers the Commissioner to audit credit information files and credit reports held by credit reporting agencies and credit providers.

7. The experience elsewhere is that an audit arising through a complaint handling process is often viewed as an adversarial compliance procedure. Privacy compliance audits and auditors have been seen by many in the past in a purely negative manner. As organizations mature in their overall approach to privacy compliance they are seeing the role of a privacy compliance audit as a process that can bring educational benefits to the organization and its staff. To many of the organizations, the outcome from an audit process seeks to educate rather than punish.

PROVISION OF THE PRIVACY COMPLIANCE AUDIT

8. The smart Identity Card scheme has attracted considerable attention from Members and the general public. Building public confidence and gaining acceptance of the scheme, particularly in relation to the non-immigration applications, is a challenge to the Administration. The PCO take note of the Administration's undertaking to commission PIA studies at various stages of the implementation so as to ensure all potential privacy issues are identified. To extend on this basis and to further enhance public confidence in the matter, the PCO support the view that the conduct of a post-implementation compliance audit is a necessary step to ensure all relevant safeguards are in place and all privacy issues duly addressed. It is also the PCO's view that subsequent regular compliance audit will be conducive to the maintenance of public confidence in the smart card regime as a whole.

9. There are distinct advantages in engaging an independent body to undertake a privacy compliance audit although it is entirely feasible that in-house audit resources of the Immigration Department may be used. In the context of public sector audits, an independent approach is much preferred as it lends impartiality and objectiveness to the audit process. This may be critical in maintaining public trust and confidence.

10. In the case of the smart Identity Card scheme, there may be two approaches to the provision of the PCA services:

a) **Engaging independent professional auditors.** This approach requires the commissioning of PCA studies with professional audit firms with the necessary privacy audit skills and experience. Although the skills required to undertake a PCA may vary with the context in which it is undertaken, the general requirements of a privacy auditor encompass a mixed set of skills in auditing, information process management, and applications of data protection principles. Depending on the scope of the audit, legal knowledge or specialist knowledge in information technology may also be needed. If deemed necessary, the PCO may assist in the selection of the privacy auditor or may approve the appointment of the auditor. The audit assignment should be carried out with a view to having the auditor submitting an audit report to the Privacy Commissioner.

b) **Appointing the PCO as an independent auditor.** Subject to the provision of additional resources to the PCO, this may be an alternative to achieve independence in the audit process. A drawback in this approach is that such appointment may create potential conflict between the PCO's role in the audit and its role in complaint investigation under the PD(P)O. To minimize the impact, a memorandum of understanding may need to be drawn up between the parties to the effect that any

outcome of the audit should not prejudice any other regulatory power of the Privacy Commissioner to enforce compliance.

11. Members have suggested for consideration the incorporation in the ROP Amendment Bill a duty of the Privacy Commissioner to carry out privacy compliance audit specifically for the smart Identity Card scheme. With due respect, the PCO have reservation about this suggestion. The PD(P)O governs both public and private sector organizations. It defines personal data in a generic manner that makes no distinction on whether an individual's identity data are more important than say the individual's health data. The Privacy Commissioner's duty under the PD(P)O is to uphold the protection of personal data regardless of the nature of data or the types of organization that are at issue. In discharging his duty, the Privacy Commissioner allows no disparity treatment to occur simply because one type of data is perceived to be more important or the concerned organization is a government department. In that context, there is no justification to accord *special* treatment to smart Identity Card data.

12. In our view, a feasible approach is to incorporate the audit requirement as a provision in a code of practice that governs the smart Identity Card scheme. This approach has the benefit that clear ground rules on the collection, use and access of smart Identity Card data can be developed in parallel with the implementation of the scheme and in tandem with development in technology. It is more flexible and allows a progressive development of the audit criteria and benchmark data. This is something that is not possible to specify at this stage. The audit criteria are important aspects of the audit process, particularly so when applying them to future non-immigration applications that might be included in the smart Identity Card. The code of practice should be a government-wide code applicable to all government departments that may be users of the smart Identity Card data, with such applicability, either in whole or in part, extendable to non-government users. If required, the Privacy Commissioner may approve the code pursuant to section 12 of the PD(P)O so as to give it a legal backing.

13. Members have also suggested that any audit report on the smart Identity Card scheme should be made public and, as a routine matter, should be tabled at the Legislative Council. On this point, the PCO have no particular view. Subject to appropriate protection of certain privileged information, the suggestion can achieve transparency in the audit process. However, it should also be noted that the Privacy Commissioner has power under the PD(P)O to publish an inspection report in the manner as he thinks fits. This would include making the report public where there is a public interest justification.

CONCLUSION

14. The PCO welcomes the opportunity to provide the above information regarding privacy compliance audit for Members' reference. We are in support of the audit requirement in respect of the smart Identity Card scheme. We believe that it would be in the interest of all parties concerned to provide such requirement as part of a government-wide code of practice, the compliance of which should be subject to the inspection power of the Privacy Commissioner under the PD(P)O.

Office of the Privacy Commissioner for Personal Data
23rd October 2002

U:/kitty/LegCoAudit(v2).doc