LC Paper No. CB(2) 217/00-01(01)

Information paper on
11 November 2000

Panel on Security of the Legislative Council
Progress of the HKSAR Identity Card Project – Privacy Issues

INTRODUCTION

At the LegCo Panel on Security Meeting held on 24 October 2000, Members were informed of the various measures to be adopted by the Government to protect the data privacy of ID card holders. This paper provides further information on the views of the Privacy Commissioner for Personal Data (Privacy Commissioner) on this subject and how his views have been addressed.

PRIVACY COMMISSIONER'S VIEWS

2. Immigration Department has been maintaining close contact with the Privacy Commissioner from the outset of the project, and obtained valuable views from him. His views have been taken into account in formulating the various data protection measures as set out in our supplementary note of 24 October 2000.

3. The Privacy Commissioner's concerns can be summarized as follows -

(a) with increasing automation and less face-to-face contact for service application and delivery, identity theft using stolen or misplaced ID cards could become a major problem;

(b) if the new ID card could be used for multiple applications, card holders should be free to choose the applications on offer. It should be a voluntary and non-discriminatory choice; and

(c) the richness in data on card may lead to function creep where data would be used for purposes beyond those for which the data were collected.

PROPOSED DATA PROTECTION MEASURES

4. As indicated in our supplementary note of 24 October 2000, we will take the following measures to address the Privacy Commissioner's concerns.

Identity Theft

5. When compared with the existing ID card, the new smart ID card will be a more effective deterrent against identity theft because the card will incorporate state-of-the-art security features on the card face and be personalized by using laser engraving technology, making it not possible to produce a counterfeit card or to alter the card face. In addition, the same set of data, together with the template of the card holder's thumbprints, will be stored in the chip. All sensitive data stored in the chip will be encrypted. The thumbprints in the chip can be used to authenticate the identity of the card holder and the chip data can be used to cross check the integrity of the data printed on the card face, when necessary. Only the rightful card holder will be able to use his own ID card.

Data Concentration and Informed Choice

6. To avoid data concentration on card, we will ensure that only minimum data is held on the new ID card. More sensitive data will, as is the present practice, be stored in the back-end computer systems. Data for different applications on card will be segregated in a secure manner by using techniques such as firewall. Since data on the card will be encrypted, only authorized persons can have access to the appropriate data/applications on the card.

7. It is envisaged that for the great majority of non-immigration applications to be offered, card holders will be given a genuine and non-discriminatory choice, the one exception being driving licence. This is because the use of driving licence is often accompanied by the need for authentication. Merging of the two will bring greater convenience to the card holder.

8. To enable card holders to know what data are stored on the smart ID card, self-service kiosks will be installed so that, after a simple process of authentication, they can view the data stored on the card.

Function Creep

9. Concerns relating to function creep is based on the premise that the issue of a smart ID card will lead to data concentration on card and common use of personal data. This will not be the case. Firstly, the collection, storage, use and release of personal data must comply with the law, in particular, the Personal Data (Privacy) Ordinance. The law must continue to be observed. Existing code of practice in relevant departments will be reviewed and refined where necessary. Secondly, as mentioned in paragraph 6, only minimum data will be held on the new ID card. Data in the back-end computer systems will, as is the present case, remain segregated and no central data bank will be established. In accordance with existing policy, the departments concerned will only collect the data which they are authorized to do so. Thirdly, stringent system access control will continue to be implemented to ensure that user departments can only have access to their own database and there will be no sharing of data. Fourthly, advanced technology will be employed to protect the integrity of data at hardware, software and application levels.

CONCLUSION

10. The Government is committed to protecting the data privacy rights of individuals. On the advice of the Privacy Commissioner, Immigration Department has contracted specialists to conduct a Privacy Impact Assessment with a view to including the necessary safeguards in the new ID card system. More Privacy Impact Assessments will be conducted at different stages of the project from the planning stage to the post implementation stage. The Privacy Commissioner will be informed of the findings of each assessment and his views will be taken into account as data protection measures are formulated or upgraded. The relevant laws will be observed at all times. This will guarantee that adequate privacy safeguards are in place.

Security Bureau
9 November 2000