PAPER TO BILLS COMMITTEE ON
REGISTRATION OF PERSONS (AMENDMENT) BILL 2001
MEETING ON 11 OCTOBER 2002

Registration of Persons (Amendment) Bill 2001

INTRODUCTION

Prior to the tabling of the Registration of Persons (Amendment) Bill 2001 before LegCo, we had opportunities on two occasions to provide to the Immigration Department ("ImmD") our comments on the proposed Bill. In particular, in September 2001, we were consulted by the ImmD on parts of the Draft Drafting Instructions then being prepared. Again, in December 2001, we were consulted by the ImmD on parts of the then draft Bill.

2. In July 2002, we were invited by the Bills Committee on Registration of Persons (Amendment) Bill 2001 to present our views on the said Bill, especially concerning the protection of personal data privacy. Subsequently, we had the opportunity to meet with representatives from the Information Technology and Broadcasting Branch of the Commerce, Industry and Technology Bureau ("CITB"), the Immigration Department, the Security Bureau and the Leisure and Cultural Services Department ("LCSD") to gain further understanding about the currently proposed non-Immigration applications of the smart ID card.

3. Given that the proposed non-Immigration applications of the smart ID card are not reflected in the Bill itself to any significant degree, our comments below will be divided into two parts, namely, those concerning such proposed applications, and those concerning the provisions of the Bill.

PROPOSED NON-IMMIGRATION APPLICATIONS

4. Our comments on the proposed non-Immigration applications of the smart ID card are necessarily based on the information provided to us about those applications. In this regard, we have been informed by the CITB that, at the present stage, the smart ID card is intended to carry the following non-Immigration applications: e-Cert, driving licence, library card and change of address.

5. Of these, we have been told, it is only the e-Cert application that will entail the storage of new data in the smart ID card (and as such, need to be mentioned in the ROP Regulations, under the new Schedule 5). This is so because, in the case of the driving licence application, the relevant driving

licence information will be kept at the Transport Department's backend computer, the smart ID card being used only as a key by means of which such data may be retrieved (say, by a police officer checking on a driver on the road, to whom the driver is under a statutory duty to produce his driving licence for inspection on demand). Similarly, information about an individual's ownership of a library card will not be stored in the smart ID card. After the introduction of the smart ID cards, individuals may request a linkage to be established between their ID card number and their library card data at the LCSD backend computer.

6. On the basis of the above understanding, the following are our preliminary observations on the proposed non-Immigration applications of the smart ID card, generally as well as with regard to each specific application:

(a) general

As for the driving licence and library card (or perhaps other future) applications, we note that the storage of the relevant data in the backend computer of the respective department may have the advantage of minimizing security risks, which would otherwise arise naturally from data concentration, if the data were stored in the smart ID card itself.

However, the proposed arrangement may give rise to a different concern, in that different entities (currently Police and LCSD) will, for the purpose of their own application, have access to the common compartment of the smart ID card which contains identification data (i.e. ID card number, Chinese and English names, data of birth and data or issue). Given this, and taking into account also the fact that the smart ID card, although physically held by the card holder, is legally owned by the ImmD, and all data are loaded onto the card by the ImmD, it is obvious that the situation will be one in which multiple parties will have access to and/or control over the same data on the card at different times. This unusual situation may create potential difficulty in applying the protection afforded by the Personal Data (Privacy) Ordinance to personal data kept in, or accessible through, the smart ID card.

In view of this, to give comfort to card holders, one may consider whether the ROP Ordinance may spell out with greater clarity the extent to which the ImmD, as the principal controller, shall be responsible for the security of data stored in the common compartment that would provide shared access by different entities.

(b) e-Cert

Given that a citizen is expected to carry his ID card with him wherever he goes, one might therefore query whether the inclusion therein of his e-Cert, being an extremely important document, may create unnecessary security risks, e.g. loss or impersonation, unless security is to be reinforced by means of additional safeguards such as biometrics.

(c) driving licence

Given that a driver is in any event under a statutory duty to show his driving licence to a Police officer on demand, and given the public safety considerations, we have no strong objection to making the smart ID card one means to retrieve the holder's driving licence data. This is so especially since we are given to understand that the choice will remain available for a driver to be issued, and to carry with him, a conventional driving licence, hence the use of his smart ID card for the driving licence application my be said to be "voluntary" at least to that extent.

(d) library card

Since the smart ID card contains sensitive invisible and visible data, the latter including the ID card number printed on the card face, the use of the card for the (rather ordinary) library card function may give rise to the question as to whether any convenience thus gained will sufficiently outweigh the data security risks involved.

In this connection, to ease any public concern and to enable a citizen to make his choice as to whether to establish a link between his smart ID card number and his library card data on an informed basis, it will be important, in offering such choice to the citizen, to explain to him any protection to be given to his data against security hazards (human or otherwise) in the course of using the smart ID card in lieu of an ordinary library card when accessing library facilities.

(e) change of address

According to the information provided to us by CITB, it seems that the change of address function on the smart ID card relates only to those individuals who have chosen to include that e-Cert on the smart ID card (which is optional for the card holder). On this basis, we have no particular comments on this application.

SPECIFIC COMMENTS ON PROVISIONS IN BILL

7. In addition to the above, we have the following comments on the specific provisions of the Bill:

(a) Clause 13

In our letter to the Immigration Department dated 1 December 2001, on Regulation 11A as proposed under Clause 10 of the then draft Bill, concern was expressed by us regarding the circumstances under which, and the manner in which, the holder of a smart ID card may be compelled to provide his thumb- or finger-print to a police officer, an officer of ImmD or an authorized person (who, we were then told, would be a member of another law enforcement agency) who has reason to doubt the identity of such holder.

Noting that Clause 13 of the current Bill is identical to Clause 10 of the earlier draft Bill, it appears that our earlier concern may not have been adequately addressed. We therefore suggest that further thought be given to the precise circumstances under which a citizen may be compelled to provide his thumb- or other finger-print (which, after all, may be regarded as much more privacy-intrusive than the mere production of one's ID card).

(b) Clause 15

According to paragraph 5 of the LegCo Brief dated 20 December 2001 presented by the Security Bureau, the amendment to Regulation 18(1) proposed under this Clause is merely to extend the existing duty on the part of a citizen to report corrections to cover non-visible data contained in a smart ID card (and, as such, may be regarded as an amendment of a consequential nature). This, however, draws one's attention to the existing Regulation 18(1) itself, the justification for which may be open to question.

In particular, we note that under the current Regulation 18(1), a citizen is under a duty to report to a registration office any changes to particulars previously submitted to a registration officer. Under Regulation 4(1)(b), such particulars include, *inter alia*, items like the citizen's residential and business address in Hong Kong, his profession, occupation, trade or employment, etc, such being items susceptible to changes from time to time (which changes, as it happens now, often go unreported). According to section 19(1), however, any person who without

reasonable excuse fails to report such changes strictly speaking commits an offence.

As a matter of actual practice, we have not been aware of the said Regulations being enforced by the ImmD with full rigour. In any event, on principle, it seems questionable whether there is any real need for the ImmD to keep such a full and updated record of the residence, place of business, employment, etc. of **all** ID card holders in Hong Kong. Unless justification can be shown for the ImmD to collect the personal data of citizens on such an extensive basis, otherwise, one should perhaps consider revising the reporting requirement under Regulation 18(1), to the extent consistent with actual need (if any), and with data protection principle 1(1) of the Personal Data (Privacy) Ordinance. (Principle 1(1) requires that personal data shall not be collected by a data user except for a purpose directly related to a function or activity of the data user, and that the data collected shall not be excessive in relation to such purpose.)

CONCLUSION

8. Generally speaking, from the point of view of the Personal Data (Privacy) Ordinance, the legal requirements which may be regarded as being of particular relevance to the current proposals regarding the smart ID card are those of data protection principles 4 and 5, which deal respectively with security in the storage and transmission of personal data, and with the availability of information regarding the policies and practices, etc., adopted by a data user in relation to personal data.

9. Indeed, in the situation of the smart ID card, the two principles mentioned above seem to be inter-related, in the sense that insofar as society as a whole may wish to avail itself of the convenience and economic benefits afforded by technological innovation, there may need to be a harms test whereby the said benefits may be balanced against potential drawbacks, including security risks, if any. On the level of the individual, in order that the offering of any choice to such individual may be meaningful, this should be accompanied by all essential information, the availability of which information, incidentally, will also help to alleviate any unnecessary concern. Given this, it is our view that it is important for the general public to be provided with a comprehensive and comprehensible picture of the proposed arrangements regarding the smart ID card. This remains a major challenge for the Administration.