LC Paper No. CB(2) 214/00-01(01)

LegCo Panel on Security
Saturday, 11 November 2000

The Proposed Smart ID Card

by
Stephen LAU
Privacy Commissioner for Personal Data, HKSAR

The new ID Card, proposed by the Hong Kong SAR Government, will serve not only to identify the individual, but also to have value-added applications built into the Card. These applications are intended to enhance the efficiency and delivery of government services as well as to provide community benefits, such as convenience and access. The indications are that the Card will contain substantial amounts of personal data, e.g. personal particulars including biometric attributes which uniquely identify the individual, and other personal data required to support the various applications. The concentration of personal data, some deemed to be sensitive, on a single card raises potential problems of data privacy which are briefly reviewed in this paper.

IDENTITY THEFT

In the information age, with increasing automation and significantly less face-to-face contact for service application and delivery, identity theft using stolen or misplaced cards would increasingly be a major problem, as evidenced in the US where identity theft is on a steep increase with the advent of the Internet and electronic commerce.

DATA CONCENTRATION, SENSITIVITY AND ACCESS

The Card with its capabilities to support the various applications can be regarded as quite a comprehensive personal dossier. While portability of the Card can be an advantage to the holder, it also can make the embedded personal data accessible to many, thus diminishing protection of the individuals' data and privacy. Richness in data tends to lead to "function creep", where data would be used for additional purposes beyond those original ones of data collection. The "function creep" in government activities tends to be justified on the basis of public interest, e.g. crime detection, welfare cheats etc. If personal data were to be used subsequently for purposes beyond those original ones of data collection, such possibilities could constitute or be perceived as an invasion of personal data privacy.

It is relevant to point out that, with the Government's announcement of this major initiative, the community has expressed considerable concerns on its potential privacy risks, including some public comments critical of this initiative as a move towards an increasingly surveillance-prone society. Given such concerns, in my view, the planning, design and implementation of the new ID Card system should have the following considerations:

1. **Privacy Impact Assessment (PIA)** should be conducted as an integral part of the planning and development of this project. PIA is an assessment of any actual or potential effects that the activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated.

   I am pleased that our on-going dialogue with the Hong Kong SAR Government has induced the recent engagement by the Government of a consulting company to conduct the initial Privacy Impact Assessment of the Smart ID Card with a view to incorporating adequate privacy safeguards into the system. I am obviously interested in the findings and recommendations of this consultancy study, and Government's views on such recommendations.

   I take note of the Government's assurance to LegCo "that every necessary measure would be taken to ensure that the right of individuals to preserve the privacy of their personal data is protected in accordance with law", and that further Privacy Impact Assessment studies will be conducted at various stages of the project.

2. The design and implementation of the new ID Card system should consider the following **privacy and fair information practice principles** to afford data protection in a modern society:

Openness	*The citizens should know their inherent rights when using the Card, what information the Card contains and how it will be used.*
Information Self-Determination	*The citizens should be aware of, for each application, what personal data the Card contains and who has access to it.*
Informed Choice	*As privacy is a very personal matter, therefore, where appropriate, the citizens should be free to choose the applications on offer. In other words, subscription to the applications should be voluntary.*
Non-discrimination	*The information on the Card, should not limit government services offered to him or be a condition for him to have access to government services; services offered through the Card should respect the universal coverage of government programs. However, it is evident that participation, although voluntary, may provide cardholders specific advantages, e.g. access outside of normal office hours.*
Security	*Adequate security features including appropriate hardware, software, encryption of data and administrative measures are required to prevent unauthorized or accidental access to and disclosure of data in the Card and personal data in the related application databases, to preserve data confidentiality, integrity and accuracy.*

Right of Access and Correction	*The citizens should be provided with the means to access, print, and interpret the data on their Cards and their personal data in the application databases, and if relevant, request for correction.*

3. Given the openness principle, different mechanisms should be considered by the Government to further assure the trust and confidence of the community to subscribe to the applications to be offered with the smart ID Card.

As an appropriate measure, it is strongly suggested that based on the privacy and fair information practice principles an administrative **code of practice** should be developed, to provide specific and clear guidelines to Government departments, for the collection, retention and use including disclosure of data in the Card and the application databases.

I would welcome the Government, on the development of this code of practice, to work jointly with my Office, which, under the Personal Data (Privacy) Ordinance, has the power to develop, solely or jointly, endorse and enforce a code of practice with regard to the protection of data privacy within an industry, profession or an activity.

In conclusion, I will continue to monitor and maintain a dialogue with the Hong Kong Government on the development of this important community-wide initiative to ensure our citizens' data privacy is adequately protected.

The Office of the Privacy Commissioner for Personal Data
8 November 2000