LC Paper No. CB(2)73/02-03(01)

Registration of Persons (Amendment) Bill
LegCo Bills Committee's Hearing
LegCo Chamber - 11th October 2002

Skeleton Submission

Opening

1. Honorable members of LegCo, I am Matthew Lee, a Barrister and a Professor of information Systems from the City University of Hong Kong. I have already made a written submission to the Bill's committee. It is not my intention today to repeat every point I have already submitted. I will just use this oral submission opportunity to emphasize a few pertinent aspects and add a couple of new points.

Key Issue

2. The smart ID scheme provides Hong Kong with an opportunity to lead the world in the provision of e-business infrastructure and e-government services. The resulting benefits for efficient and responsible government, our economic transformation, and enhanced citizen convenience are issues I do not dispute. But at the same time, the scheme also entails a certain degree of risk to all residents of Hong Kong since virtually every person in Hong Kong above the age of 10 will be required by law to register for and carry the new smart ID card. The risk is that the smart ID card, once extensively used for all purposes, may enable the government and other personal data users to use the card as a means of abusive social

control and massive invasion of privacy. This is the evil we must guard against.

3. The Bill contains several new provisions to guard against the unauthorized disclosure and use of ROP data. There is also a provision to safeguard the integrity of data on the chip from the risk of unlawful tampering. The questions are whether these provisions are sufficiently adequate given the nature of risks involved, and whether the provisions can be effectively enforced in practice.

The Proposed Amendments

4. The usage restrictions contained in S.9 are apparently clear and specific. ROP data can only be used for the three purposes stipulated in S.9. However, on a closer examination, the legislative intention and interpretation of S.9 leave me in some doubt. In my view the stated purposes should be better qualified. In particular, the stated purposes should not be used as a means for achieving other ulterior purposes. For example, S9(b) says ROP data may be used to enable the identification of individuals - but in order to do what? If identification is necessary for a certain purpose provided for in a corresponding piece of legislation, then it is fine. However, the ability to quickly identify individuals with certain personal or behavioral characteristics provides whosoever in control of the data with a potential means of abusive social control and privacy invasion on a large scale. If the purpose of enabling identification is to facilitate other ulterior purposes not authorized by law, such identification should be prohibited. I would urge honorable members of this Council to consider tightening up the wordings of S.9(b) to prevent such a mischief.

5. The new S.10 imposes a statutory duty on a registration officer not to disclose ROP data. That seems fine. The problem is that the same provision also gives the Chief Secretary for Administration an unfettered discretion to permit the disclosure of ROP data to any person or organization. Under this section, the Chief Secretary does not need to account for the use of his discretion al all. If fact, the public (or LegCo members for that matter) will not even know whether the Chief Secretary has exercised his discretion, let alone questioning the grounds on which such discretion is made. Unfettered executive discretion without any degree of judicial control is dangerous and will do nothing to increase citizens' trust on the Government or allay citizen's fear of privacy abuses. Although this discretion has long been with us (under the existing Regulation 24), it takes on added significance in the era of smart ID cards and e-government wherein it is expected that a lot more personal data will be collected and held in government and other organizational databases and ROP data will become instrumental in linking and matching personal data in these databases to construct individual profiles. I would urge honorable members to consider amending S.10 so as to put some limitation on this discretion or to subject the exercise of this discretion to some reasonable checks and balances.

6. The new S.11 criminalizes the unlawful handling of ROP data. This section is much welcome as it will provide some deterrence against threats to the privacy and security of ROP data. To some extent it offers some protection against the unfettered discretion of the Chief Secretary to disclose data under S.10 because the party receiving the disclosed ROP data will still be restricted by S.11, unless that party is outside our jurisdiction. However, if one does not even know whether and, if so, to whom the Chief Secretary has disclosed ROP data pursuant to S.10, it

will be hardly possible to enforce S.11 against the receiving party in practice.

7. The amended Regulation 12(1A) criminalizes the unlawful tampering of the memory content of the chip on an ID card and the chip itself. This section is much welcome as it will provide some deterrence against threats to the privacy and security of both ROP and non-ROP data held in the chip. However, there is a glaring omission – the provision does not cover unauthorized access, so called "hacking", to data held in the chip. Hacking presents a real threat to privacy and security no less than unlawful tampering of data in the chip. This is especially so given that S.9 to S.11 offer protection to ROP data only. Regulation 12(1A) is therefore the only provision for the protection of non-ROP data held in the chip. Since the Chief Executive in Council can in future quite easily add other non-ROP applications and data to the chip through amending Schedule 5, it is quite reasonable to expect the chip to contain more and more non-ROP data in the future. Even if the adoption of non-immigration applications by the users is optional, convenience and usefulness will eventually dictate adoption. Leaving out the hacking offence is therefore dangerous and inconsistent with the general approach taken in our computer crime legislation. In my view, hacking personal data on the smart ID card presents an even more serious threat to privacy, security and public confidence than general hacking *per se*. There is no reason to leave this offence out from the amendment. I would urge honorable members of this Council to consider revising the amendment to include this important measure to strengthen the legal safeguard against threats to privacy and security.

Ensuring Compliance

8. The deterrence effect provided by the new SS. 9-11 and Regulation 12 will be seriously compromised if a breach of the relevant provisions cannot be detected. For this purpose some kind of privacy audit should be performed on a regular basis to identify weaknesses in the operation of the ROP systems, processes and policies, and point to any non-compliance that may in turn lead to further criminal investigation to be instituted. To ensure impartiality and credibility, privacy audit should be carried out by an independent 3rd party (preferably under statutory authority). In Australia, their statutes provide for privacy audits on federal agencies to be carried out by the Privacy Commissioner. This is perhaps an approach that honorable members of this Council may want to consider. Whether this should be done by amending our Privacy Ordinance in general (so as to affect all governmental personal data controllers) or amending the ROP Ordinance in particular (to affect only the immigration department) will of course require further deliberation.

Closing

9. In closing I would like to emphasis that the proposed amendments are necessary and broadly in the right direction and they should in principle be supported. I have pointed out a number of important privacy and security issues that the amendments have apparently failed to address, and to which I would urge honorable members to pay particular attention. It is in our public interest to reap without delay the enormous potential social and economic benefits brought about by e-government and a deepened e-business technology infrastructure enabled by the smart ID card. At the same time we must guard against the evil of abusive social control and unwarranted privacy invasion. The legislature surely has an important role to play in this critical juncture. My oral submission has

now come to the end. I shall be glad if I could be of further assistance. Thank you.

Matthew Lee
9th October 2002