Bills Committee on Registration of Persons (Amendment) Bill

Submission on the smart ID Card and the Registration of Persons (Amendment) Bill 2001

28 October 2002

Professor Graham Greenleaf
University of Hong Kong Faculty of Law
<g.greenleaf@hku.hk>

Contents

1 Summary

1.1 Summary of main arguments

This Submission replaces and expands upon my Summary Submission dated 18 July 2002[1], and replies to points raised in the Administration's Response to that submission (hereinafter 'Administration Response to Greenleaf')[2]. I adhere to most points that I raised previously, as I detail in this Submission.

The principal submissions I wish to make may be summarised as follows:

- The core problem of the Hong Kong ID system is that its purpose has never been defined with precision, and its expansion into a smart-card-based system is exacerbating that problem by being based around an intended but undefined expansion of functions. With the introduction of the smart ID card, it is the appropriate time for LegCo to provide more precise definition.
- The Administration describes the four initial proposed uses of the smart ID card as 'voluntary'. I argue that 'quasi-voluntary' is a more accurate description. Irrespective of whether we call them 'voluntary', such proposed uses still require close LegCo scrutiny of the whole context in which the changes will operate, and whether they are in the public interest or involve dangers. In each of the four initial non-immigration applications, there are matters that require LegCo's attention.
- Existing provisions, and the proposed amendments to the ROP Ordinance and Regulations give LegCo a very weak degree of control over the expansion of uses of the smart ID card and its associated number and database, with risks of LegCo control being bypassed once the system is established. A list of proposed amendment to the ROP (Amendment) Bill 2001 are suggested to overcome this weakness and re-assert more democratic control over the development of the ID system.
- If there is greater ease of electronic capture of ID numbers and other basic identity information such as name, the smart ID card may dramatically increase the collection and retention of ID numbers and their use to link internal organisational data. The fact that there will be a separate segment on the ID card chip for 'card face data' (ID number, name, data of birth and data of issue) increases the risk that private sector and public sector bodies could be allowed to use card readers to capture this data. At present, the only protections against this occurring are technical protections (readers must be able to authenticate to the card), and the very weak controls over use of the ID number in the Personal Data (Privacy) Ordinance and the Commissioner's Code. I suggest that the ROP Ordinance should also prohibit any uses of card readers except those approved by regulations subject to positive LegCo approval.
- I submit that the Administration should be required by the ROP Ordinance to provide to LegCo a Privacy Impact Assessment (PIA) for each proposed additional

---

1 LC Paper No. CB(2)2620/01-02(01) (English version issued on 18.7.2002, Chinese version issued vide LC Paper No. CB(2)2785/01-02 on 17.9.2002) - Submission from Professor Graham GREENLEAF

2 LC Paper No. CB(2)21/02-03(01) (issued on 7.10.2002) - Administration's response to the points raised in the submission from Professor Graham GREENLEAF (LC Paper No. CB(2)2620/01-02(01)) <http://www.legco.gov.hk/yr01-02/english/bc/bc56/papers/bc561011cb2-21-1e.pdf>

use of the ID card or number. Furthermore, the terms of reference for the PIA(s) should require approval by LegCo, to ensure that all implications are canvassed.

- I submit that the ROP Ordinance should be redrafted as a comprehensive code controlling all aspects of Hong Kong's ID system, as recommended by the first Privacy Impact Assessment (PIA). Details are suggested of what should be covered.
- Taking into account the constitutional position of the Hong Kong SAR and the world-wide volatility of ID systems following September 11 2001, it is appropriate for Hong Kong to take a very cautious approach to any proposals for the expanded uses of an ID system. The current proposals involve many protective measures, but they are not yet sufficient.

1.2 List of recommendations submitted

The following recommendations are submitted to LegCo in the course of this paper:

- With the introduction of the smart ID card, it is the appropriate time for LegCo to provide more precise definition of the circumstances under which government agencies collect the ID number, retain it, and correlate it with other records that they hold.
- LegCo must ensure that it retains the ability to prevent any extensions of the use of the ID system, whether they can be labelled 'voluntary' or not.
- Where new uses or functions are to be added to the card and/or the chip, positive LegCo approval under Interpretation and General Clauses Ordinance (IGCO) s35 is preferable to s34 disallowance.
- The Bill should define precisely which classes of persons can be made 'authorized persons' under ROP Reg 11A, and that any expansion of that potential class of 'authorized persons' should only be made by Regulations and therefore subject to LegCo approval.
- New uses of the ID card or number which can be brought in without any legislative changes should also require positive LegCo approval.
- It would be better if new uses of the ROP database, under the new ROPO s9, also required s35 positive LegCo approval, and were not only subject to disallowance.
- New forms of disclosure from the ROP database by the Immigration Department to external organisations, defined by class of persons, should only be made by Regulations (not merely approval in writing), and thereby made subject to LegCo scrutiny.
- The existing protections preventing unauthorized uses of card readers should be strengthened by amendments to the ROP Ordinance prohibiting any uses of card readers except those approved by regulations subject to positive LegCo approval.
- To avoid any doubt, the new ROPO s11 should state that 'particulars' includes any information stored on the ID card.
- The Administration should be required to provide a Privacy Impact Assessment (PIA) for each proposed additional use of the ID card or number; the ROPO should be amended to require this and to further require that (i) the terms of reference for the PIA(s) should require approval by LegCo, to ensure that all implications are canvassed, including whether or not the application should be an allowed use of the ID card; (ii) the approval of the Privacy Commissioner be required to the particular consultant that the Administration proposed to appoint, to ensure that the

consultant had appropriate privacy expertise; and (iii) the Administration be required to publish the PIAs in sufficient time to allow public comment.

- The ROP Ordinance should be redrafted as a comprehensive code controlling all aspects of Hong Kong's ID system.
- LegCo should take a very cautious approach to all aspects of the possibility of expansion of the ID system, due to the untested mix of elements in the new ID system, and the position of the HK SAR as part of the PRC.

2 An ID system designed to have no limits

2.1 Lack of definition of the ID system's purposes

The core problem of the Hong Kong ID system is that its purpose has never been defined with precision, and its conversion into a smart-card-based system is exacerbating that problem by being based around an intended but undefined expansion of functions.

To illustrate the second point, ITBB pointed out in 2001 that '[t]he potential use of the chip is large and new possible functions are emerging all the time' [3]. At various time, uses that have been under consideration include general access to government services, e-voting, health records and an electronic purse. More recently, ITBB has pointed out that the separate 'card-face data' segment will give 'flexibility', and will allow 'case by case' approval of other applications for the purpose of 'authenticating citizens before services are provided'[4].

One reason that this undefined potential range of uses of the ID card is possible in the public sector is because the Registration of Persons Ordinance (ROPO) s5(1)(b) provides that, not withstanding any other law to the contrary, a person 'in all dealings with government' shall furnish his ID card number where required. As a result, the Privacy Commissioner's Code does not impose limits on the collection of ID numbers by government agencies[5]. It also allows the ID numbers to be used as multi-purpose internal identifier by any organisation[6].

In the private sector, the Privacy Commissioner's Code also places few limits on the routine collection of ID numbers (though they cannot compel disclosure) by any organisation that requires some reliability of identification in order to avoid non-trivial losses[7], and allows such numbers to be used as multi-purpose internal identifiers by the organisation. At present the main protection against more extensive use of ID numbers by the private sector is the difficulty of collecting ID numbers by automated means.

The longer-term risk of ID system expansion are summarised by Prof. Matthew Lee[8]:

> '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 ITBB LegCo Panels briefing Non-immigration Applications for Incorporation into the Smart ID Card (20 Dec 2001)

4 ITBB 'Update on non-Immigration Applications for Incorporation into the Smart ID Card', 4 July 2002,

5 Privacy Commissioner *Code of Practice on the Identity Card Number and other Personal Identifiers*, 1997, para 2.3,.1

6 Privacy Commissioner *Code of Practice on the Identity Card Number and other Personal Identifiers*, 1997, para 2.3 and particularly para 2.3.3.3

7 Privacy Commissioner *Code of Practice on the Identity Card Number and other Personal Identifiers*, 1997, para 2.6.3

8 Submission from Professor Matthew LEE [CB(2)2785/01-02(02)] (11 October 2002) , para 2

I submit that, with the introduction of the smart ID card, it is the appropriate time for LegCo to provide more precise definition of the circumstances under which government agencies collect the ID number, retain it, and correlate it with other records that they hold. It is also the appropriate time for LegCo to re-assess the use of the ID number by the private sector.

It may not be possible for LegCo to define now all possible future uses of the ID card and number which should be allowed as in the public interest. However, it is possible for LegCo to institute legislative changes which will give it sufficient control over all subsequent changes to the ID system to ensure that a definition of what uses are in the public interest will emerge from subsequent LegCo examination of new proposed uses.

2.2 Claimed 'voluntariness' of non-immigration uses is no answer

The Administration claims that all proposed non-immigration uses are voluntary. This is correct (and desirable) in the limited sense that it is not compulsory to have extra information on the ID card, and the four applications can be achieved by other means. I argue in the Appendix that in relation to each proposed use, the extent of 'voluntariness' significantly limited or qualified, either in that citizens/consumers will not remain unaffected by new uses even if they ostensibly opt out of them, or in that they are not being given a genuinely non-discriminatory choice. In my opinion, these three proposed uses are better described as 'quasi-voluntary'. I agree with Prof Matthew Lee's comment that '[e]ven if the adoption of non-immigration applications by the users is optional, convenience and usefulness will eventually dictate adoption'[9].

Irrespective of whether we call these proposed uses 'voluntary', the more important point is that close LegCo scrutiny of the whole context in which the changes will operate, and whether the proposed uses are in the public interest or involve dangers, is still needed. The label of 'voluntariness' does not answer the question of whether an additional use of the ID card should be allowed, either for these proposed uses or any in future. I submit LegCo must ensure that it retains the ability to prevent any extensions of the use of the ID system, whether they can be labelled 'voluntary' or not.

The four initial proposed new uses are discussed in the Appendix, to illustrate how LegCo needs to consider the whole context, and why it should ensure it has the power to approve all proposed new uses. My comments are not necessarily criticisms of the four proposed applications, but more of the need for changed processes.

3 Inadequate LegCo controls over expansion of the ID system

Existing provisions, and the proposed amendments to the ROP Ordinance and Regulations give LegCo a very weak degree of control over the expansion of uses of the smart ID card and its associated number and database, once the system is established and the Bill passed.

The weaknesses in LegCo's ongoing control, and its dangers, are detailed in the following.

3.1 New uses of the card and/or chip

- New uses or functions can be added to the card and/or the chip merely by amendment to Schedule 5 ROP Regulations[10], not the ROP Ordinance. These changes do not require positive LegCo approval under Interpretation and General Clauses Ordinance (IGCO) s35, but only the weaker s34 provision for disallowance.

---

9 Submission from Professor Matthew LEE [CB(2)2785/01-02(02)] (11 October 2002) para 6

10 See ROP (Amendment) Bill cls 7.10 and 21

It is quite possible that a new use of the card/chip might not require amendment of any other Ordinance[11]. I submit s35 positive approval would be preferable.

- The use of card readers to do ID checks (including fingerprint comparisons) is open to any 'authorized persons' approved by the Chief Executive (new Reg11A), by notice published in the Gazette. Such notices are not subsidiary legislation[12], so there is no LegCo scrutiny of the exercise of this power. The Administration claims[13] that 'it is necessary to allow the Chief Executive the flexibility to order other "authorized persons" (law enforcement officers) to perform the same task so that he can deal with emergency situations ...'. Elsewhere they say 'The term "authorized persons" is intended to mean law-enforcement officers. Private sector will not be given any such power.' The defect in this claim is that Reg 11A nowhere refers to 'law enforcement officers' or places any restriction on who can be an 'authorized person'. This legislation needs to be very specific on who can be authorized to fingerprint and ID-check Hong Kong SAR residents. For example, could private sector security guards, or some mainland government officials, be made 'authorized persons'? I submit that the Bill should define precisely which classes of persons can be made 'authorized persons', and that any expansion of that potential class of 'authorized persons' should only be made by Regulations and therefore subject to LegCo approval.
- If a new government use of the card does not require additional data on the card, no Schedule 5 change is needed, and therefore there is no LegCo opportunity for scrutiny. New uses of the card can arise if any government agency decides to use the card in replacement for some identification card of its own, relying on the power to require a person to furnish their card number when dealing with government (ROPO s5). In some cases of government uses there will be some coincidental change to other legislation which is needed (as occurred with the need to carry a driver's licence, and the library card application), but there is no reason to expect that such coincidental changes will always be needed. The Administration states that Legco 'involvement ... will not be neglected'[14], but this avoids the more important point that it is not required. LegCo involvement should not depend on the good will of the Administration. I submit that the Administration's claim that 'legislation is only required when there is additional data on chip or when changes to the underlying legislation are necessary' should be rejected: new uses which can be brought in without any legislative changes could be just as dangerous as those that do require legislative changes, and the potential expansion of the uses of the ID system is in not tied to changes of the card or chip. They should also require positive LegCo approval.

3.2 Controls on uses of the ROP database

- The consultants in the first Privacy Impact Assessment set out why the ROP Database is now more attractive to external users because of its expanded digital content[15], a point also raised by Prof Matthew Lee in his submission[16]. New uses of the ROP database (in the sense of uses by the Immigration Department itself) can be authorised by any Ordinance or Regulation (new s9 ROPO)[17]. They also only require

---

11 Administration Response to Greenleaf 4.1 obscures this point by assuming that all non-immigration applications will require some 'separate legislative exercise'. There is no basis for this assumption.

12 New ROP Regulation 11A(4)

13 Administration Response to Greenleaf 4.4

14 Administration Response to Greenleaf 4.3

15 See <http://www.legco.gov.hk/yr00-01/english/fc/esc/papers/esc27e1.pdf>

16 Submission from Professor Matthew LEE [CB(2)2785/01-02(02)] (11 October 2002) , para 5

17 New s9 of ROPO - See ROP (Amendment) Bill

s34 disallowance. The new s9 is a privacy-positive step[18], but I submit that s35 positive LegCo approval would be a further improvement and one that is justified by the significance of what is being approved.

- In contrast, new forms of disclosure from the ROP database by the Immigration Department to external organisations only require approval in writing from the Chief Secretary (new s10 ROPO), with no LegCo scrutiny at all[19]. The Administration has implemented commendable privacy-protection practices under the existing Regulation 24[20], in order to implement the PD(P)O's restrictions on disclosure of personal information. The problem is that s10 allows the Chief Secretary (by his delegate, the Secretary for Security) to authorise disclosures by a 'class or category of persons by name, office or description'. In the case of such disclosures by broad class of persons, I question whether the essentially after-the-event protections of the PD(P)O (in the absence of any audit power in the Commissioner) is sufficient. I submit that such disclosures by class of persons should only be made by Regulations, and thereby made subject to LegCo scrutiny, and the ability of the Commissioner to make submissions to LegCo. This matter approaches the seriousness of data-matching, which requires special approval under the PD(P)O , and should also be subject to special procedures.

In summary, under the ROP (Amendment) Bill, LegCo control of the expansion of the ID system could be largely bypassed once the system is in place. I submit this is inappropriate and that the Ordinance and Regulations should be amended to provide an appropriate level of LegCo control over all of the above matters.

4 Potential increased use of ID number needs more control

The collection of the ID card number in Hong Kong is already largely uncontrolled. It is allowed for almost any self-protective uses, and it can then be used as an internal identifier within organisations, except for restrictions on transfers of ID numbers between organisations (which is generally prohibited)[21]. New uses of the card and number in the private sector can arise whenever a private sector body requires card production for the purpose of correct identification to protect against non-trivial harm[22], and then uses the number as the basis of its internal identification system. As discussed above, new uses can also arise in the public sector. Private sector bodies cannot compel a person to furnish their number (unless authorized by law)[23], but it is clear that they can and do legitimately request it in many circumstances.

In this context, the introduction of the smart ID card would be very likely to dramatically increase the collection and retention of ID numbers and their use to link internal organisational data, *if* it brought with it greater ease of electronic capture of ID numbers and other basic identity information such as name.

This potential risk is heightened by the existence of the 'card face segment'. There will be a separate segment on the ID card chip for 'card face data' (ID number, name, data of birth

---

18 This is the main point of Administration Response to Greenleaf 4.2 - I agree.

19 Administration Response to Greenleaf 4.2 misses the point, by not addressing the lack of LegCo scrutiny.

20 Administration's paper "Provision of Registration of Persons records" LC Paper No. CB(2) 150/02-03(01) <http://www.legco.gov.hk/yr01-02/english/bc/bc56/papers/bc561028cb2-150-1e.pdf>

21 This is a summary of the Privacy Commissioner *Code of Practice on the Identity Card Number and other Personal Identifiers*, 1997

22 See Privacy Commissioner *Code of Practice on the Identity Card Number and other Personal Identifiers*, 1997, para 2.3, particularly 2.3.3.3

23 See Privacy Commissioner *Code of Practice on the Identity Card Number and other Personal Identifiers*, 1997 para 2.1

and data of issue), which will be able to be accessed electronically by libraries as part of the proposed library card function, 'and on a case by case basis for other functions that may be approved in future'[24]. The chip therefore has differential levels of security for different segments.

At present, given the weak controls over use of the ID number in the Personal Data (Privacy) Ordinance and the Commissioner's Code, the only significant protections against further proliferation of use of the ID number are technical and administrative protections preventing electronic reading of the card face segment. The Administration points out[25] that there are both technical and administrative safeguards:

> 'only authorised card-reading devices with the appropriate cryptographic keys can read the personal data in the chip of the smart ID card. Any party intending to access the information must first obtain approval from the Government as well as the consent of the card holder.'

Furthermore, the new s11 ROPO will create an offence where anyone 'without lawful authority or reasonable excuse, gains access to, stores, uses or discloses, any particulars furnished to a registration officer'. The Administration's view, which may be correct[26], is that particulars in the card face segment would be 'particulars furnished to a registration officer', and so unauthorised reading of card face data will be prohibited[27]. To put this beyond doubt, I submit that the new s11 should state that 'particulars' includes any information stored on the ID card.

These technical, administrative and legal protections are all valuable, but they still allow the possibility that the Administration could authorise any private sector or public sector party to use card readers (with the appropriate cryptographic keys) to read and capture card face data. The weak controls in the PD(P)O and the Commissioner's Code would have little effect on this. Regulation 11A, referred to by the Administration[28], seems beside the point, as it only deals with production for fingerprint verification, not for the simpler purpose of reading card face data.

This matter should not be left to administrative discretion. I submit that the existing protections should be strengthened by amendments to the ROP Ordinance prohibiting any uses of card readers except those approved by regulations subject to positive LegCo approval.

5 Privacy Impact Assessments needed for non-immigration uses

The Immigration Department (ImmD) obtained an initial Privacy Impact Assessment (PIA) on the immigration uses of the change to a smart card, an edited version of which has been made available to the public [29]. The Immigration Department has now released a second PIA (to LegCo but not yet available on the web[30]). The first PIA explicitly did not deal with non-immigration uses of the card/number. The Administration claims that the

---

24 ITBB 'Update on non-Immigration Applications for Incorporation into the Smart ID Card', 4 July 2002

25 Administration Response to Greenleaf 5.1

26 Prof Matthew Lee seems to doubt this in relation to ROP data as well as non-ROP data,; he observes that non-ROP data is not protected here,: para 7 of Submission from Professor Matthew LEE [CB(2)2785/01-02(02)] (11 October 2002)

27 Administration Response to Greenleaf 5.1; I had neglected this provision in my Summary Submission.

28 Administration Response to Greenleaf 5.1

29 <http://www.legco.gov.hk/yr00-01/english/fc/esc/papers/esc27e1.pdf>

30 An Administration summary and response is available in Administration's paper entitled "HKSAR Identity Card Project - Latest Developments and the Second Privacy Impact Assessment Report" [CB(2)2433/01-02(07)] (10 July 2002) <http://www.legco.gov.hk/yr01-02/english/panels/se/papers/se0710cb2-2433-7e.pdf>

unpublished second PIA has already addressed the privacy aspects of the non-immigration applications'[31].

From the available summary, it appears that the second PIA does address some operational and public perception issues in relation to non-Immigration applications[32]. However, the consultants comments appear (from the summary) to proceed on the assumption that the non-Immigration applications will all go ahead, and if so what can then be done to minimise the privacy dangers [33]. They do not address the prior question of whether each application should be a use of the ID card at all, and what are the privacy or other risks in inclusion.

I submit that the Administration should be required to provide a PIA for each proposed additional use of the ID card or number, and that the ROP Ordinance should be amended accordingly. Furthermore, the terms of reference for the PIA(s) should require approval by LegCo, to ensure that all implications are canvassed, including whether or not the application should be an allowed use of the ID card. It would also be desirable if the approval of the Privacy Commissioner was required to the particular consultant that the Administration proposed to appoint, to ensure that the consultant had appropriate privacy expertise. The Administration should also be required to publish the PIAs in sufficient time to allow public comment before LegCo assesses them.

The need for comprehensive PIAs has been supported by Dr John Bacon Shone at the Symposium on the smart ID Card in May 2002, and by Prof. Matthew Lee in his oral evidence to LegCo.

It is possible that there may be many more proposed applications of the ID card and number, and it is desirable that LegCo should implement a better process by which it can approve or disapprove proposed expansions on the basis of comprehensive, expert and independent Privacy Impact Assessments.

6 A comprehensive code for the ID system is needed

I submit that the ROP Ordinance should be redrafted as a comprehensive code controlling all aspects of Hong Kong's ID system, as recommended by the first Privacy Impact Assessment (PIA)[34]. The Administration claims it has already done this[35], but it has not.

The numerous further amendments recommended in this submission, and in other submissions such as that of Professor Lee, show that a comprehensive code has not yet been achieved. A comprehensive code could also involve a re-assessment by LegCo of:

- how and when government agencies require ID numbers under s5 of the ROPO, and what further use they make of them
- the controls on private sector collection and use of the ID number, in light of the new circumstances of the smart ID card;
- the operation of ROPO Regulations 4 and 18, in light of the new circumstances of the smart ID card.

---

31 Administration Response to Greenleaf 2

32 Summary of second PIA, paras 9, 10 and 12

33 eg para 9: 'Privacy concerns would be minimised if ...'

34 First PIA, p60

35 Administration Response to Greenleaf 5.3

7 Caution in ID expansion is appropriate in Hong Kong

ID systems are an important element in the mechanisms by which States exercise control over populations. Fully democratic political systems have more checks and balances by which potential abuses of ID systems may be prevented. Expansions of ID systems carry a lower level of risk in such systems.

Factors which should be considered include that Hong Kong is part of the People's Republic of China (PRC), and although it does have a high degree of autonomy it does not have complete control over its political destiny. The PRC is not a democracy, and nor is Hong Kong a full democracy, although the Basic Law provides for it to become more democratic over time.

After September 11 2001 there is a high degree of volatility in proposals concerning ID systems worldwide. Hong Kong has not yet enacted a security law as envisaged in the Basic Law, but is considering doing so. The final content of such a security law could have a major impact on the true meaning and implications of any ID card system, and the extended uses of such a system. This aspect also requires further LegCo consideration.

When all these factors are considered, it seems appropriate for Hong Kong to take a very cautious approach to any proposals for the expanded uses of an ID system. This is particularly so when the change to a smart-card based system is in itself a major technological and social change which may have consequences and difficulties not yet foreseen.

The Administration says it is already taking a cautious approach[36]. I have no reason to doubt its good intentions, but as this submission has detailed, the current approach leaves too much control in the hands of the Executive, and not in the hands of the more democratic body, LegCo. It is not yet a cautious enough approach.

The current Hong Kong proposals are for an ID system which comprises a potent and untested mix of an identity number, name, digital photograph, smart card, digital signature, biometric (fingerprint), and PIN (for eCert). The eventual uses of the system are intentionally not defined and are intended to expand. If these proposals are to go ahead, they must be tempered by democratic controls in every aspect of their design and implementation.

I submit that LegCo should take a very cautious approach to all aspects of the possibility of expansion of the ID system, due to the untested mix of elements in the new ID system, and the position of the HK SAR as part of the PRC.

---

[36] Administration Response to Greenleaf 5.6

8 Appendix - The four initial non-immigration uses

8.1 Driver's licence on backend computer

Although there already driver's licence details stored on the Transport Department (TD) backend computer, there are more significant changes to existing practices proposed here than the Administration admits.

At present, all drivers have a physically visible plastic licence which can be inspected by Police. It is therefore not necessary in many cases for Police who have pulled over a driver to do a backend check, as they can readily establish that the person does hold a driver's licence[37], and the driver's identity (if necessary by also requiring production of ID card with photo).

Under the new system, the default position is that drivers will not have a visible licence and will have to opt-in in order to obtain one - the plastic licence. If (as seems likely) most drivers will not opt-in to obtain the plastic licence, then Police who have pulled over a driver will always need to do a backend check, as they otherwise cannot even establish that the person has ever held a driver's licence. The Administration claims that 'circumstances for checking should be no different from (not more comprehensive than) the current practice'[38]. I submit this is incorrect because it ignores that most drivers will no longer hold a visible licence.

Where a person does opt-in to obtain a plastic licence, Police checking of the backend database could still become more likely than it was before. ROP Regulation 11 will not exempt holders of plastic driver's licences from online checking. Nor does it stop Police (nor should it) from requiring production of an ID card (ROPO s5) to enable the card to be swiped, once Police are equipped with card readers that can do online checks. If this becomes commonplace then the plastic licence may become meaningless in interactions with Police, and only used for hiring cars, overseas driving, and other non-Police interactions where a visible licence is essential.

This change is only 'voluntary' if you consider that a requirement to opt-in in order to maintain the status quo is 'voluntary'. This is a compulsory change to a substantially different system. It is not necessarily an objectionable change (particularly given that Hong Kong driver's licences are already based on ID number), but it illustrates that labelling a use of the card 'voluntary' tells us little, and that the whole circumstances of a new use of the ID card should be subject to LegCo scrutiny, irrespective of considerations of 'voluntariness'.

8.2 Online change of address use

At present, use of HK Post eCert is compulsory for online change of address at ESD kiosks. The smart ID card will provide a new token on which the eCert will be carried. Use of other digital signatures at ESD kiosks may be approved[39], but has not been as yet.

Residents do have choice of informing government departments by post or personal attendance of a change of address[40], but the issue remains of whether the ID card

---

37 They cannot check if it has been suspended unless they contact the backend system.

38 Administration Response to Greenleaf 1.1

39 Administration Response to Greenleaf 1.3 says they are finalising a plan to allow signatures issued by another recognised CA, DigiSign.

40 Administration Response to Greenleaf 1.3

proposals are giving residents as full a choice of options for *electronic* change of address as is reasonably practicable. Otherwise, in order to carry out transactions in cyberspace, this application becomes less voluntary than it seems.

ITBB explicitly rejects[41] the use of PIN authentication by a PIN stored on the ID card, as a means of accessing government services, and proposes that the e-Cert use will be the only method implemented on the ID card. ITBB accepts that PIN use could be 'a user-friendly infrastructure for e-services'. However, the only reason it puts forward for rejection is that the e-Cert is capable of carrying out the job, and there are no 'suitable application(s) for adopting the PIN authentication', so the additional investment is therefore not justified. ITBB also claims that it would be difficult to explain PIN use to the public without confusion 'without an immediate use of the PIN to explain its usefulness'.

ITBB does not even discuss the online change of address use as a potential use of PINs, and does not say why online change of address use would be difficult to explain. The ITBB paper gives the impression that the decision had already been made that PINs must not undermine the viability of the e-Cert, and were not being considered seriously. There may be reasons why PINs are not suitable for a change of address application[42], but to establish this would require a comparison with the how the same result can be achieved with the more complex digital signature technology. It should be borne in mind that the level of security that is really needed for change of address may be lower for some purposes than others.

The Administration's apparent unwillingness to consider inclusion of a PIN on the ID card seems to undermines its argument that the use of the e-Cert on the ID card is 'voluntary and non-discriminatory'[43], as it appears that users will not be given as full a choice of options in electronic transactions as might be possible. A comprehensive PIA on non-immigration applications would have dealt with matters like this.

A further matter which requires consideration as part of the overall context in which the ID system operates is the role of ROP Regulation 18 together with ROP Regulation 4. Taken together, these regulations would require residents to inform the Immigration department every time they changed their residential or business address, marital status, family membership, or occupation. These regulations do not seem to be fully enforced at present, or Hong Kong would have a full family register system. If at some time in future ROP Regulation 18, requiring updating of particulars was enforced fully, then for anyone who wanted the convenience of online updating, there would be no choice but to use the e-Cert. These factors should be considered by LegCo, perhaps as part of a more general consideration of Regulations 4 and 18 as part of developing a comprehensive code for the ID system.

8.3 Library card use

Leisure & Cultural Services Dept. (LCSD) will be able to read/copy electronically from the chip all data on the face of the card ('card face data')[44]. No other proposed application requires reading only that data. The library application is the first of what may be many other applications for 'authenticating citizens before services are provided' based on reading card-face data, and it is very important for that reason. Without the library application, there would have been no current need to design a card with a separate card

---

41 ITBB 'Update on non-Immigration Applications for Incorporation into the Smart ID Card', 4 July 2002, paras 12-15

42 See the article by Pun et al in the Hong Kong Law Journal [current issue, citation to be added] for arguments about problems with PINs

43 Administration Response to Greenleaf 1.3

44 ITBB 'Update on non-Immigration Applications for Incorporation into the Smart ID Card', 4 July 2002

face segment. By adding what ITBB describes as the 'straight-forward and non-controversial' library application, the basis for many possible extended uses has been designed in to the Card from the outset.

The Administration says that the library card application 'has been designed to use the ID card number as a matching key to the library card number'[45]. This increases the risk that a person's library borrowings (sensitive information[46]) could become known to others because it is easier to find out a person's ID number than their library number. No doubt security measures have been taken to prevent this from eventuating, but the risk has been increased through correlation with another numbering system.

The extent of the risk of matching keys depends on whether LCSD holds a person's ID number as a key irrespective of whether they choose to use the plastic library card instead (in which case they would be at higher risk even though they had not 'volunteered'). It seems that this application will only be 'voluntary' in the weaker 'opt-out' sense because 'library users will have the option to be issued with plastic library cards'[47]. This question deserves clarification. It does not appear to be discussed in the second PIA.

As Dr John Bacon-Shone has noted[48], there is no need for the ID number to be used as the library number: if the library card number was stored on a separate component on the card, providing the convenience of dispensing with a separate library card, without the dangers of expanding use of the ID number into another information system. The Administration considers this would be more costly and could involve some inconvenience if an ID card was lost or remote services were being used[49], and has rejected this alternative on these grounds. This option does not seem to have been considered in the second PIA[50].

This example illustrates how LegCo has to consider the full context of even a 'straight-forward and non-controversial' application, and the cost-benefits of alternatives, before deciding whether it is justified.

8.4 HK Post eCert on the chip

The 'deep infrastructure' ITBB and HK Post are aiming for appears to be close to the position of a monopoly government provider of digital signature to consumers. No case has been made out for the inclusion of signatures on the card beyond the 'convenience' of having one card for various functions. This is not sufficient justification, as it involves risks which the Administration is ignoring.

The Administration says it will 'consider allowing digital certificates by recognised certification authorities (CAs) ....other than HKPost' on the ID card 'when there is strong public support'[51]. This ignores two vital matters: (i) there is no evidence of 'strong public support' for a government-provided digital signature on the chip; and (ii) no other CA provider will ever be given the opportunity to ask all SAR residents whether they agree to

---

45 Administration Response to Greenleaf 1.4

46 A person's borrowings of books or films can indicate a person's beliefs and interests. In the USA specific legislation has been enacted concerning the privacy of video rentals.

47 ITBB LegCo Panels briefing Non-immigration Applications for Incorporation into the Smart ID Card (20 Dec 2001), para 17; see also Administration Response to Greenleaf 2

48 Presentation at Symposium on the smart ID card, May 2002.

49 Administration Response to Greenleaf 1.4

50 See details in paras 9-10, Administration's paper entitled "HKSAR Identity Card Project - Latest Developments and the Second Privacy Impact Assessment Report" [CB(2)2433/01-02(07)] (10 July 2002) <http://www.legco.gov.hk/yr01-02/english/panels/se/papers/se0710cb2-2433-7e.pdf>

51 Administration Response to Greenleaf 1.2

have their company's digital signature on the chip. The 'first mover advantage' to HKPost is such that it should be able to achieve something close to a monopoly position in relation to the provision of general-purpose digital signatures. The lack of an unfair trade practices law in Hong Kong does not mean the government should give legislative endorsement to such practices. This is particularly so when an effective monopoly increases the privacy dangers.

The privacy dangers of digital signatures on ID cards are largely matters of future possibility, and it is not suggested they are matters of current policy or intent:

- One type of privacy danger of digital signatures on a government ID card arises from abuses of government power in breach of the law. Examples are (i) a government obtaining access to the private key; or (ii) a government capturing data relating to digital signature use.
- Other types of problem would require legislative changes. Examples are (i) if a government made available a compulsory ID biometric (eg fingerprint template) to be used in substitution for a PIN needed to access the digital signature segment (this would increase the spread of biometric identification in a potentially dangerous ways by using it to link two key identifiers, ID number and digital signature); or (ii) a government requiring that an ID number always be used in conjunction with a digital signature, or vice-versa, in electronic transactions.

These potential dangers are less if there are multiple signature providers. The likelihood of collaboration in abuses is greatly reduced by the number of parties required. The likelihood of effective opposition to undesirable legislative changes by signature providers is greater the more providers are involved. *A fortiori* when some of the providers come from the private sector, and have less incentive to comply with government wishes than a government provider.

The Administration will no doubt say that these things will not happen. It is probable that they will not, but they are the type of plausible potential dangers which can best be reduced by allowing multiple signature providers (or by not having signatures on the ID card at all).

The Administration claims that to allow for signatures from multiple CAs on one card would raise 'more issues on privacy protection'[52]. Another way of putting it is that the Administration would have to get the protective measures right at the outset. After all, if it is genuinely contemplating allowing signatures from other CAs in future, it needs to ensure now that the chip architecture can deal with this.

The provision of only the e-Cert on the chip is therefore unjustifiably discriminatory, and does not allow citizens the full choice that should be available to them, contrary to Administration assertions[53].

It is true that e-Certs (and other certificates) are available on other media. However, can we have confidence that during the process of issuing the smart ID card every eligible person in Hong Kong will be fully informed of and fully understand all of the alternatives available to them concerning digital signatures and other authentication options? The organisation informing them will be one signature vendor, HK Post, that has a unique opportunity to sell its product. It is unrealistic to expect that they will fully and fairly explain the alternatives. In theory, citizens are free to choose, but in practice they may make an uninformed choice.

---

52 Administration Response to Greenleaf 1.2

53 Administration Response to Greenleaf 1.2

A further factor to take into account is that, if the use of a digital signature is ever made the only practical option in other contexts (eg for online multiple change of address - discussed above), this reduces the extent of voluntariness in holding an e-Cert on the smart card. Voluntariness is a matter of degree, here as elsewhere.