

Summary submission concerning the 'smart' ID Card

=====

and the Registration of Persons (Amendment) Bill

=====

Please see my attached Powerpoint presentation 'Hong Kong's New ID Card: Smart Bits and Risks' (presented at the Symposium of that name at the University of Hong Kong on 22 June) as part of this submission. Major points are summarised below, but some further details are in the slides.

1 Proposed non-immigration uses not truly voluntary

The Information Technology and Broadcasting Bureau (ITBB), as proponent of the non-immigration uses of the smart ID card, has claimed that all proposed uses are voluntary. As detailed in my Powerpoint slides, I argue that this claim is questionable in relation to each proposed use, in that citizens/consumers will not remain unaffected by new uses even if they ostensibly opt out of them, or they are not being given a genuinely non-discriminatory choice. These proposed uses are better described as 'quasi-voluntary' or 'pseudo-voluntary'.

1.1 Driver's licence on back-end computer

This aspect is compulsory, and comprehensive Police checking remains likely (ROP Reg11 will not exempt holders of plastic driver's licences).

1.2 HK Post eCert on the chip

The 'deep infrastructure' ITBB and HK Post are aiming for is a monopoly government provider of digital signature to consumers. The lack of an unfair trade practices law does not mean the government should endorse such practices. The privacy dangers of digital signatures are less if there are multiple providers. If use of a digital signature is compulsory in other contexts (eg online multiple change of address), this makes the obtaining of an eCert on the smart card only 'pseudo voluntary'.

1.3 Online change of address use

At present, use of HK Post eCert is compulsory for this, and the smart ID card will continue this requirement, merely providing the token on which the eCert will be carried. The latest ITBB paper on non-Immigration uses

(June 2002) explicitly rejects the use of PIN authentication as a means of accessing government services, and proposes that eCert use will be the only method accepted. There is clearly no real choice here. (see implications above). Further, if ROP Reg18, requiring updating of particulars (address, occupation, family status), was enforced then this use would also become pseudo-voluntary, as convenience would dictate use.

1.4 Library card use

As Dr John Bacon-Shone has noted, there is no need for the ID number to be used as the library number. Real choice would allow the library card number to be 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.

2 Lack of Privacy Impact Assessments 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, and edited version of which has recently been made available to the public (see <http://www.legco.gov.hk/yr00-01/english/fc/esc/papers/esc27e1.pdf>). ImmD has now released a second PIA (to LegCo but not yet available on the web). The first PIA explicitly did not deal with non-immigration uses of the card/number, and my understanding is that the second PIA does not do so either.

The Information Technology and Broadcasting Bureau (ITBB), as proponent of the non-immigration uses, has not commissioned PIAs on any of the expanded uses it proposes. As Dr John Bacon-Shone noted at the recent Symposium, the significance and implications of such uses require a PIA, and ITBB should be required to follow the good example of ImmD. My comments above concerning the pseudo-voluntary nature of the proposed uses are among the issues that a PIA would address.

I submit that ITBB 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.

3 Dangers of increased use of ID number by private sector, other agencies

The collection of the ID card number in Hong Kong is already largely uncontrolled (being allowed for almost any self-protective uses), as is its use as an internal identifier within organisations, except for restrictions on transfers of ID numbers between organisations (which is generally prohibited). This is a summary of the position under the Privacy Commissioner's 'Code of Practice on ID Card Numbers and other Personal Identifiers' (see slides).

The smart ID card may dramatically increase the collection and retention of ID numbers and their use to link internal organisational data, particularly if there is greater ease of electronic capture of ID numbers and other basic identity information such as name.

The latest ITBB paper on non-Immigration uses (June 2002) confirms 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), 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'.

The chip therefore has differential levels of security for different segments, making it very likely that electronic capture of 'card face data' will proliferate, and therefore the uses of the ID number.

4 LegCo not being given adequate control over expansion of this 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. These weaknesses include (see slides):

- * New uses can be added to the card/chip merely by amendment to Sched 5 ROP Regs, not the Ordinance. These do not even require positive LegCo approval under Interpretation and General Clauses Ordinance (IGCO) s35, but only the weaker s34 provision for disallowance.
- * New uses of the ROP database (now more attractive though its expanded

digital content, as the first PIA consultants correctly insist) also only require s34 disallowance.

* New forms of disclosure from the ROP database only require approval in writing from the Chief Secretary (new s10), with no LegCo scrutiny at all.

* If a new use of the card does not require additional data on the card, no Sched 5 change is needed, and therefore there is no LegCo opportunity for scrutiny (unless some coincidental change to other legislation is needed).

* 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), and there is explicitly no LegCo scrutiny of this (new Reg11A(4)).

In summary, LegCo control of the expansion of the ID system will 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.

It would be preferable if the ROP Ordinance was redrafted as a comprehensive code controlling all aspects of Hong Kong's ID system.

5 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 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.

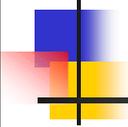
When all these factors are considered, it seems appropriate for Hong Kong to take a very cautious approach to any proposals for the expanded uses of an ID system, particularly in the context of where a change to a smart-card based system is in itself a major technological and social change which may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

The 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. This is a time for caution, not rash experiment.

Graham Greenleaf

Distinguished Visiting Professor (2001-02)
Faculty of Law, University of Hong Kong
Pokfulam Road, Hong Kong (Room 502, KK Leung Bldg)
Office HKU Tel: +852 2859 2931 Fax: +852 2559 3543

Professor of Law
Faculty of Law, University of New South Wales
UNSW SYDNEY NSW 2052 Australia (UNSW CRICOS Provider No: 00098G)
Co-Director, Australasian Legal Information Institute (AustLII)
Co-Director, Baker & McKenzie Cyberspace Law and Policy Centre



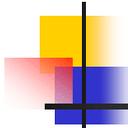
Hong Kong's New ID Card: Smart Bits and Risks

Professor Graham Greenleaf

Faculty of Law

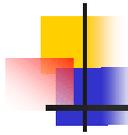
University of Hong Kong

22 June 2002



An ID system is not just a card

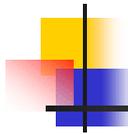
- A set of identifiers
 - Number + photo + thumbprints etc
- Token (Card)
 - Carries identifiers + data + processor
- Database(s) - ROP and others
- Collection points
 - Readers + requirements to produce
- Communications
 - Between tokens, readers and databases



The multi-purpose 'dumb' ID card

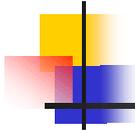
Privacy Commissioner Code of Practice on the ID Card Number - his interpretation of the PDPO

- ID numbers may be **collected** with few limits:
 - for all dealings with government
 - by anyone wherever 'present or future correct identification is necessary' to prevent harm to the cardholder or anyone else, including non-trivial loss to the card user
- **Copies** of cards may be required to verify identity remotely



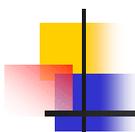
Uses of the 'dumb' ID (II)

- ID numbers may be used as the index of any internal record system - it is a **multi-purpose internal identifier**
- ID numbers may be **shared** by organisations where collected for 'a purpose shared by both' (otherwise, disclosure/matching generally prohibited, unless approved by PCO)
- The 'smart' ID card may facilitate **expansion** of all these existing uses



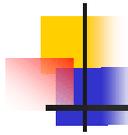
Question about uses

- Are the initial non-immigration uses truly 'voluntary'?
- What further use expansion is anticipated?
- What controls will there be on expansion of uses of the ID system? (not only the Card)
- Will the risks of a multi-purpose ID be minimised?
- Are the risks of a multi-purpose ID justified?



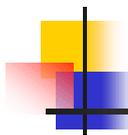
'Voluntary' extra uses?

- "None of the applications ... is compulsory" (ITBB)
- but only re information embedded in the card
- **Driver's licence** on backend computer
 - Compulsory change to online licence
 - Additional plastic licence is voluntary
 - Comprehensive online checking likely
 - If Police have readers, will they 'type not swipe'?
 - ROP r11 does not exempt plastic licences



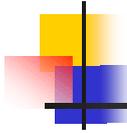
'Voluntary' extra uses? (II)

- **HK Post E-cert on the chip**
 - At card issue, public will be required to choose whether or not to have E-cert on chip
 - 'A unique opportunity ... to create a deep infrastructure' - and free for the first year too
 - No choice of which digital signature - HK Post only
 - Is a monopoly government digital signature more dangerous as a cyberspace ID?



'Voluntary' extra uses (III)

- **Online change of address**
 - Only possible with HKPost E-cert as yet
 - Is this really a 'non-discriminatory choice'?
 - What if ROP r18 was enforced, to require updating of address, occupation, family status etc?
 - Should ROP r18 drop most updating?
- **Library card**
 - HKID number on chip to access library services
 - Users must opt-out by requesting plastic card



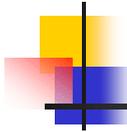
Anticipated function creep

- “the potential use of the chip is large and new possible functions are emerging all the time” (ITBB)
- Uses considered included general access to government services, e-voting, health records and an electronic purse
- Chip has capacity to add many other functions
- But many functions do not require additional storage on the chip
 - No significant control of private sector uses
 - Online collection of ID numbers will facilitate realtime surveillance, matching and retention

28/10/2002

Graham Greenleaf, HKU

9



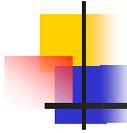
Controls on uses: card/chip

- The **card (and chip)** can have new data / functions added
 - merely amend Sched 5 ROP Regs
 - disallowable by LegCo (IGCO s34)
 - no positive LegCo approval (IGCO s35) needed
 - see Registration of Persons (Amendment) Bill 2001, (ROPA) cls 7, 10 and 21

28/10/2002

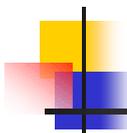
Graham Greenleaf, HKU

10



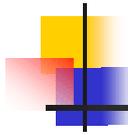
Controls on uses: Database

- The ROP **database**
 - Will now be far more attractive to other users
 - Can be *used* as authorised by any Ord/Reg (new s9) - only s34 disallowance, not s35 LegCo approval
 - Can be *disclosed* as Chief Secretary permits (new s10) - any procedures for LegCo scrutiny?
 - Is *protected* by offences of unlawful access (new s11)



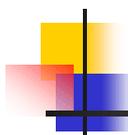
Controls on uses: Other uses

- Some new uses of card/database will not require any legislation
 - If no additional data on card, no Sched 5 change needed
 - If only needs disclosure of registration data, Chief Secretary can authorise
 - Drivers licence and library applications only require amendments to other Regs *by coincidence*
 - Does online change of address use require legislation?
- Should all uses require s35 Legco approval?



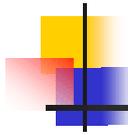
Uses: Official card access

- Which officials will have readers? Why?
 - Police, Immigration and 'authorized persons' can use readers to do ID checks, including against card biometrics (fingerprints) (new r11A)
 - No LegCo scrutiny of creation of 'authorised persons' by Chief Executive (r11A(4)).



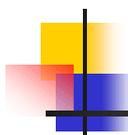
Uses: Other card access?

- Will non-officials be able to use readers?
 - No *legal* prohibition on others scanning the digital ID number from the card - *technically* possible?
 - R 11A allows private sector 'authorised users'
 - Scannable ID numbers could massively increase retention and internal use of ID numbers
 - Altering card content is prohibited, but not reading (new r14)
- Individual access
 - Kiosks to allow individuals to check card contents
 - Can individuals use readers at home?



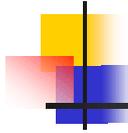
Uses and protections

- Protections are mainly aimed at misuse and security, not at limiting use
 - The PD(P)O does not fill this gap
- LegCo's control of uses is limited
 - Positive (s35) approval not needed
 - Some forms of expansion are outside LegCo scrutiny
- There is no comprehensive legal regime for this ID system



Justifications

- see [LegCo Brief](#)
- Justifications for a **smart** card
 - Fraud prevention and convenience
- Justifications for a **multi-purpose** card
 - 'a unique opportunity'
 - Convenience in 'one card for various functions'
 - HK 'should not lag behind' other countries ('Finland, Malaysia')
 - Separation of ID card and multi-purpose card dismissed



Longer-term considerations

- No inherent limits: Planned 'function creep'
- Multi-purpose cards raise the risks
 - Cancellation of multiple rights possible
 - Risks of identity theft may be higher
 - Aggregation of separate personal data
- ID card + chip + digital signature (E-cert) may become a 'cyberspace passport'
 - uses may become compulsory (by law or de facto)
- Long-term dangers of repressive use should not be ignored - caution makes sense