Hong Kong Special Administrative Region
Identity Card Project

Initial Privacy Impact Assessment

Report

Submitted September 2000

Revised after Client comments, November 2000

Pacific Privacy Pty Ltd

12A Kelvin Grove
Nelson Bay
NSW 2315 Australia
(02) 4981 0828

CONTENTS

EXECUTIVE SUMMARY

This report assesses the privacy implications of the proposed HKSAR ID Card scheme.

In order to understand the way in which the proposed new system will work, and the extent of any changes, it was necessary to review the existing HK ID Card system. Accordingly, Part II of the report describes the current scheme, while Part III describes the proposed scheme.

Identity card systems, and the population registers associated with them, can be particularly sensitive in privacy terms. They bring together issues of personal data privacy with wider issues relating to the privacy of the person, of communications, and of behaviour, and the extent to which individuals are monitored – by the state and by private sector.

Sensitivity varies between jurisdictions. In some countries, including some in east Asia, proposals for new or upgraded ID card systems have provoked fierce controversy, while in others sophisticated ID Card schemes have been accepted with little apparent concern. An overview of international experience is included in Part IV and Appendix 5. Part IV also introduces some other contextual material including a legal analysis and a review of research findings.

In Hong Kong, the existing ID Card, and its widespread use in both public and private sectors, appear to have been accepted without major concern. The privacy-intrusive potential of the Card has however been limited by several factors; notably the lack of easy access to registration information, and the fact that the information is generally not kept up to date.

The Immigration Department's proposals of the new HKSAR ID Card, in relation to its own functions and activities, are modest and do not involve significant new uses. Nevertheless, several aspects of the proposed new Card and its supporting infrastructure have significant privacy implications. The use of a smartcard with 'invisible' data, the inclusion of a digitized biometric (thumbprint) and the consequent use of card receiving devices all change the nature of the scheme in ways which some people will see as threatening to privacy. In the consultants' judgement, the easier access to 'imaged' registration data is also likely to lead to greater use of that information by other agencies, which in turn could lead to pressure on ImmD to maintain a more up-to-date population register. Such a development would be very significant in privacy terms.

If the new HKSAR ID Card is designed to support other applications, even if those applications have yet to be decided, then a range of other privacy issues arises. While there is uncertainty about what other applications might be added to the card, there will be a level of concern about the potential of the Card to lead to an increase in the degree of monitoring, surveillance and data linkage – all of which are significant privacy issues.

Public attitudes to any further uses of the ID Card, or to the use of multi-application smartcards, are unknown – survey research would be valuable. An informed public debate about the privacy implications of the scheme – balanced against its other benefits and costs, would also be desirable. Without such a debate at an early stage there is a risk that privacy concerns, which may in part be based on uninformed speculation, could become a major inhibitor later in the development of the project.

There are many practical steps that can be taken to reduce the privacy risk associated with the proposed scheme. Many of these take the form of technical specifications which can be built in to the design. In some cases this has already been done. Some legislative amendments and procedural changes will also be necessary; to provide for the new elements of the scheme, to ensure compliance with the Personal Data (Privacy) Ordinance and to ensure that confidentiality provisions are comprehensive and enforceable. The risks involved, and the steps suggested to address those risks, are explained in Part V.

The Report does not make specific recommendations. It is up to the Immigration Department to decide how to address the privacy risks that are identified, particularly in light of its timetable for implementation of the HKSAR ID Card.

Pacific Privacy Pty Ltd
18 September 2000

PART I – GENERAL BACKGROUND & CONTEXT

Context

The Immigration Department (ImmD) of the Hong Kong Special Administrative Region (HKSAR) has conducted a feasibility study (FS) on the future HKSAR Identity Card. It is now moving to the System Analysis and Design stage.

The proposed enhancement of the HK ID card is to involve a re-registration of the entire population of some 6.8 million people, and the issue of a new smart card storing both traditional identification and demographic details, and biometrics (digitised photo and thumbprints).

The new ID Card will be used, as the current card is, for identification in a wide range of interactions with government and the private sector. In addition, consideration is being given in a separate inter-departmental initiative to a range of extra applications to be included in a government smart card, such as replacing existing driving licences and library cards; electronic cash storage for electronic service delivery transactions with government; and digital signatures. Other potential applications include health records and commercial uses.

Some of these applications could be included on the new ImmD-issued ID card, and although decisions are not likely to be made for some time, ImmD is being asked to provide capacity and functionality for a range of additional applications in the specifications for its new card.

Subject to policy approval and funding, the new Identity Card System will go live in late 2002 or early 2003 to replace the current system. In order to meet this timetable, a request for tender, incorporating major design parameters, will need to be issued early in 2001.

The Department has identified privacy as a significant issue, and has engaged Pacific Privacy Pty Ltd to conduct an initial Privacy Impact Assessment (PIA), to be completed in time to be taken into account in drawing up the request for tender for the new card and associated infrastructure. The FS Report recommended three further PIAs at later stages of the implementation plan, but the timing and specification of these are subject to review.

Privacy Impact Assessments

The concept of a Privacy Impact Assessment (PIA) has been emerging gradually in jurisdictions with privacy or data protection laws[1] [2]. Essentially, it means a systematic appraisal of the privacy implications of a new proposal. Some appraisals are limited

[1] See paper by Blair Stewart, Assistant Privacy Commissioner, New Zealand, in *Privacy Law & Policy Reporter* 1996, (PLPR), 1996, Vol 3 p 61, & p134. (access via www.austlii.edu.au)
[2] See Clarke, R. *Privacy Impact Assessments*, at http://www.anu.edu.au/people/Roger.Clarke/DV/PIA.html

to assessing compliance with specific privacy rules or standards, but others range more widely over all privacy issues of concern to affected individuals, whether or not they are currently subject to privacy law. The concept of a PIA owes much to the well-established tool of Environmental Impact Assessments (EIAs).

PIAs differ from privacy audits in that audits are generally after-the-event assessments of how an organisation is complying with existing rules. PIAs are prospective - they assess how a proposal would comply with rules, or, more commonly, what privacy issues a proposal will raise, including but not limited to compliance issues. PIAs can also identify an appropriate role for privacy enhancing technologies (PETs) which can give individuals a measure of control over their personal information.

The concept of a PIA is being adopted both in the private and pubic sectors. President Clinton's Chief Privacy Counselor has recently promoted the use of PIAs in the corporate sector[3], and the Data Protection Commissioners from around the world have discussed PIAs at many of their annual conferences.

Although no jurisdiction to date has formally adopted the term or the concept of PIAs as a statutory requirement, some have introduced versions of the concept in particular contexts. For instance, the Ontario Management Board Secretariat (MBS) requires agencies to undertake PIAs as part of their annual Information and Information Technology (I&IT) plans, to demonstrate compliance with the *Freedom of Information and Protection of Privacy Act*[4]. And the Australian *Data matching (Assistance and Tax) Act 1990* includes a requirement for agencies to draw up program protocols for proposed matching exercises which amount to PIAs.[5]

The role of a PIA for the HK ID Card

An enhanced ID card is one of the most privacy-sensitive proposals that could be put forward in Hong Kong. Although the existing ID card is a familiar and accepted feature of residency in Hong Kong, any expansion of the role of the card, to incorporate new functions or to be used in new contexts, is likely to be very sensitive. Even if the functions and context of use did not change at all, the fact that the new card will be a smart card, containing 'hidden' data; that the registration data is to be stored in a more accessible form, and that thumbprints will be required to be read in additional circumstances, would all raise privacy issues. As it is, the specifications mention not only other government uses but also the possibility of commercial applications. Even if no new applications are envisaged in the short term, public reaction to the enhancement will depend partly on analysis of the potential applications and uses, and their implications.

The privacy issues surrounding the ID card relate not only to the cards themselves and the information they carry about the bearer, but also to the acquisition and use of information on the card, both visible data and that on the chip; to the central

[3] Address by Peter Swire to Corporate Privacy Officers, June 2000 - see *Privacy and American Business* Volume 7 No 4, August/September 2000.
[4] http://www.gov.on.ca/MBS/english/fip/pia/
[5] see materials on the Privacy Commissioner's web site at www.privacy.gov.au

databases used for registration and production of the cards, and to any paper or microfilm records.

A comprehensive PIA can demonstrate clearly to the community that all of the short and long term privacy implications have been considered, and can indicate appropriate privacy and security safeguards that could be incorporated in the design of the new system. It is possible that some potential applications may be so privacy-sensitive that the Department may decide to rule them out in order to ensure the public acceptability of the scheme as a whole.

Compliance with the terms of the Personal Data (Privacy) Ordinance (PDPO) is an important part of the PIA, but it needed to range much more broadly. A PIA which focussed exclusively on compliance with the Ordinance, or even on data privacy issues alone would miss the point. The PIA will only be credible, and a useful guide to designing the new system, if it addresses the full range of privacy concerns.

Ideally, a Privacy Impact Assessment should be conducted from the outset as a public process. Involving the community in drafting the terms of reference for the PIA; allowing public input at various stages in the conduct of the Assessment, and making the findings public all maximise the credibility of the exercise. In this case, while some Information about the ID card project has been made public in connection with the Legislative Council processes in February, March and June 2000, the timetable has not allowed public input to the terms of reference or conduct of the PIA. However, the findings could be made public and input from the public taken into account, even though decisions will need to be taken before the end of the year about the design specifications.

Underlying Concepts

The purpose of this section is to define a number of technical concepts that are significant to the analysis that follows.

Human Identification

Identity is an abstract concept that refers to a specific entity, such as a particular human being or company, or a particular instance of, say, a motor car. In an information system, the abstract concept needs to be operationalised. It is defined as a set of information about an entity that differentiates it from other, similar entities. The set of information might be as small as a single code that is specifically designed as an identifier (such as the Hong Kong ID Card Number, or the Person Reference Number), or it might be a compound of such data as the person’s given and family names, date-of-birth and postcode of residence.

Human identification is the association of data with a particular human being. An organisation's identification process comprises the acquisition of the relevant identifying information. This enables new data to be associated with an identifier, and hence both an identity in the real world, and existing data already on file about that identity.

An entity does not necessarily have a single identity, but may have multiple identities. For example, a company may have many business units, divisions, branches, trading-names, trademarks and brandnames. And many people are known by different names which are associated with them only when they play a particular role in a particular context.

A variety of person-identification techniques are available, which can assist in associating data with them. Important examples of these techniques include:

- names – or what the person is called by other people;
- codes – or what the person is called by an organisation;
- knowledge – or what the person knows;
- tokens – or what the person has; and
- biometrics – or what the person is, does, or looks like.

Authentication

Authentication is the process whereby a degree of confidence is established about the truth of an assertion.

A common application of the idea is to the **authentication of identity**. This is the process whereby an organisation establishes that a party it is dealing with is:

- a previously known real-world entity (in which case it can associate transactions with existing records in the relevant information system); or
- a previously unknown real-world entity (in which case it may be appropriate to create a new record in the relevant information system, and perhaps also to create an organisational identifier for that party).

In addition, there are many circumstances in which organisations undertake **authentication of value**, e.g. by checking a banknote for forgery-resistant features like metal wires or holograms, and seeking pre-authorisation of credit-card payments.

Another approach is the **authentication of attributes, credentials or eligibility**. In this case, it is not the person's identity that is in focus, but rather the capacity of that person to perform some function, such as being granted a discount applicable only to tradesmen or club-members, or a concessional fee only available to senior citizens or school-children, or entry to premises that are restricted to adults only.

Anonymity

An anonymous record or transaction is one whose data cannot be associated with a particular individual, either from the data itself, or by combining the transaction with other data. A great many transactions that people undertake are entirely anonymous, including barter transactions, visits to enquiry counters in government agencies and shops, telephone enquiries, cash transactions such as the myriad daily

payments for inexpensive goods and services, gambling and road-tolls, and treatment at discreet clinics, particularly for sexually transmitted diseases.

Pseudonymity

In addition to identified and anonymous transactions, a further alternative exists. A pseudonymous record or transaction is one that cannot, in the normal course of events, be associated with a particular individual. Hence a transaction is pseudonymous in relation to a particular party if the transaction data contains no direct identifier for that party, and can only be related to them in the event that a very specific piece of additional data is associated with it. The data may, however, be indirectly associated with the person if particular procedures are followed, e.g. the issuing of a search warrant authorising access to an otherwise closed index.

To be effective, pseudonymous mechanisms must involve legal, organisational and technical protections, such that the link can only be made (e.g. the index can only be accessed) under appropriate circumstances.

Privacy

Privacy is the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations. Privacy is not a single interest, but rather has several dimensions:

- privacy of the person, sometimes referred to as 'bodily privacy' This is concerned with the integrity of the individual's body. Issues include compulsory immunisation, blood transfusion without consent, compulsory provision of biometrics and samples of body fluids and body tissue, and compulsory sterilisation;
- privacy of personal behaviour. This relates to all aspects of behaviour and constraints on personal behaviour, but especially to sensitive matters, such as sexual preferences and habits, political activities and religious practices, both in private and in public places. It includes what is sometimes referred to as 'media privacy';
- privacy of personal communications. Individuals claim an interest in being able to communicate among themselves, using various media, without routine monitoring of their communications by other persons or organisations. This includes what is sometimes referred to as 'interception privacy'; and
- privacy of personal data. Individuals claim that data about themselves should not be automatically available to other individuals and organisations, and that, even where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use. This is sometimes referred to as 'data privacy' and 'information privacy'.

During the second half of the twentieth century, privacy has been of increasing concern within economically advanced nations. During the 1970s and 1980s,

legislatures of countries throughout the Continent of Europe, and States and Provinces in North America, passed laws addressing information privacy. These laws mostly focus on 'data protection' or 'fair information practices'. The Hong Kong Personal Data (Privacy) Ordinance is such a law, while the Hong Kong Law Reform Commission Privacy Sub-Committee has wider terms of reference encompassing some of the other dimensions.

Privacy-Enhancing Technologies (PETs)

The term PET was coined in the early 1990s, and was first popularised in the title of a work by the Data Protection Commissioners of Ontario and The Netherlands. It refers to technologies that are expressly designed to protect people's privacy. They are most commonly mechanisms for achieving anonymity. Some, however, aim to provide individuals with control over flows of data about themselves, and some are designed to deliver pseudonymity rather than anonymity.

Privacy-Invasive Technologies (the PITs)

The term 'the PITs' was coined to refer to mainstream technologies that, at best, ignore the need for privacy, and, at worst, are specifically designed to invade privacy. Examples of PITs include video-surveillance cameras, data matching and profiling software, and national identification schemes.

Smart Cards

A smart-card is a standard-sized plastic card that contains an integrated circuit or 'chip' which gives the card the ability to store and/or process data.

Key advantages that a smart-card offers over less sophisticated cards are considerably greater security, far greater storage capacity, and the ability to provide services from a standalone unit, which is not, or is only infrequently, connected to the service's host machine. The more sophisticated smart-cards offer further capabilities, including the ability to segment the storage area and apply differential security to each area, the ability to use the same card for multiple services, and the ability to use the same card to link card-holders to multiple service-providers.

The key disadvantages of chip-card technology are the cost of the cards, the need for an external device to provide a power-supply, clock-function and (in most cases) input-output capabilities, and the cost of devices to read the cards.

Contact-based cards need to be placed quite precisely into a device that can provide at least power, and generally also a data interchange path. This approach requires that the person place the card in a device, wait, and take it out again afterwards. Contact cards suffer a considerable degree of wear, limiting the life of the card.

Since the early 1990s, contactless or 'proximity smart card' technology has also been available. Such a card needs to be close to the device with which it is to interchange data, but does not need to be in physical contact with the device. Contactless cards

communicate, using radio-frequency (RF), with another, generally stationary chip that is installed in a terminal of some kind. Power is provided by induction, as a result of an antenna on the card being moved through a magnetic field provided by the stationary device. Systems that use contactless cards need have no moving parts, which greatly reduces a major source of wear-and-tear to the card and the card-reading device. They could, however, be activated without the cardholder being aware that the card is participating in a transaction on their behalf.

Digital Signatures

A digital signature is a string of binary digits appended to an electronic message, which can reliably demonstrate to the recipient something about the sender. For example, it can authenticate the identity of the sender, or it can authenticate some characteristic or attribute of the sender, such as the ability to conduct business on behalf of a particular company, or to act as a medical practitioner.

Digital signature technology depends on asymmetric cryptography, which was invented about 1975. Digital signatures are generated using a 'private key', which only the relevant person must ever possess. They are authenticated using a 'public key', which any person who receives messages needs to have access to.

In order to be confident that a particular public key belongs to (or 'is bound to') a particular person or organisation, or signifies a particular credential, it is necessary to check with some trusted organisation. Such an organisation is called a Certification Authority (CA). A CA issues digital certificates that attest that a particular public key is that of a particular person or organisation, or signifies a particular credential.

In order for digital signature arrangements to be credible and reliable, a number of conditions need to be satisfied. These include key-generation mechanisms, key-storage mechanisms, secure digital signature generation mechanisms, means of communicating public keys and digital certificates, CAs, and processes whereby each CA is confident enough to issue certificates. This substantial collection of entities and processes is referred to as public key infrastructure (PKI).

Biometrics

The term 'biometric' is used to refer to those person-identification techniques that are based on some physical and difficult-to-alienate characteristic, such as:

- appearance – how the person looks (e.g. the familiar passport descriptions of height, weight, colour of skin, hair and eyes, visible physical markings; gender; race; facial hair, wearing of glasses; supported by photographs);
- social behaviour – how the person interacts with others (e.g. habituated body-signals; general voice characteristics; style of speech; visible handicaps; supported by video-film);
- bio-dynamics – what the person does (e.g. the manner in which one's signature is written; statistically-analysed voice characteristics; keystroke dynamics, particularly in relation to login-id and password);

- natural physiography – what the person is (e.g. skull measurements; teeth and skeletal injuries; thumbprint, fingerprint sets and handprints; retinal scans; earlobe capillary patterns; hand geometry; DNA-patterns); and
- imposed physical characteristics – what the person is now (e.g. dog-tags, collars, bracelets and anklets; brands and bar-codes; embedded micro-chips and transponders).

PART II – SPECIFIC BACKGROUND - THE EXISTING HK ID CARD SYSTEM

Brief History of the Registration of Persons and Issuing of Identity Cards in Hong Kong

The history of the registration of persons and identity card system in Hong Kong in modern times is a history of responses to crises: - responses that subsequently became embedded in everyday life and survived although the immediate crises that prompted them passed.

The current system may be traced to the enactment of the Registration of Persons Ordinance 1949. The primary objective of the legislation was to assist measures that might be found necessary for the maintenance of law and order and for the distribution of food or other commodities as a result of prevailing conditions of economic and political unrest.[6]

In introducing the legislation the Government gave a commitment that the scheme would be withdrawn when such conditions ceased to prevail.[7]

The system was overhauled in 1960 when a new Registration of Persons Ordinance was enacted. The Government took the view at that time that the registration of persons had come to be well accepted and the existence of Identity Cards was useful and valuable.[8] Indeed, there was by this time 'considerable extraneous [i.e. non-Government] use' of Identity Cards, which was cited by the Government as justification, in part, for levying an issuing fee.[9]

Neither the 1949 nor the 1960 Ordinances required registered persons to carry identity cards or other proof of identity. Such a requirement was introduced in two stages in 1979 and 1980 as a response to the crisis caused by large influxes of illegal immigrants under the 'reached base' policy of the time.

Firstly, in 1979 the Registration of Persons Ordinance was amended to empower the Governor to make regulations requiring persons to carry their identity cards in designated areas. Those regulations were duly made two days after the amending legislation was enacted and by the end of 1980 designated areas included most of the New Territories.

[6] Speech by Attorney General moving the First Reading of the Registration of Persons Bill 1949 and Objects and Reasons for the Bill, Hong Kong Legislative Council Hansard, 1949, pp.225 to 227.
[7] Op cit, p.226.
[8] Speech by the Colonial Secretary moving the First Reading of the Registration of Persons Bill 1960, Hong Kong Legislative Council Hansard, 1960, .p169.
[9] Op cit, p.170.

Then, in 1980, the Immigration (Amendment)(No.2) Ordinance was passed to make legislative changes in support of the decision to abandon the 'reached base' policy.[10] The legislation made it compulsory for all registered persons over the age of 15 to carry a recognised 'proof of identity', which as a practical matter for most people meant the identity card. This was justified as being necessary in order to enforce the provisions in the Ordinance that made it an offence to employ an illegal immigrant.[11]

In arguing for acceptance of the new requirement, the Governor recognised that having to carry proof of identity would be 'irksome'.[12] However, unlike what was said in 1949, no indication was given that the requirement might be dropped once the crisis was over.

Brief Overview of the Existing HK ID Card Scheme

Hong Kong SAR has a universal and mandatory identity card scheme. It is operated by the Registration of Persons (ROP) Office within the Immigration Department (ImmD). It is used by several Divisions within ImmD, by the Police, and by many agencies of the HKSAR government, for many different purposes.

The elements that make up the scheme as a whole are as follows:

- the card;
- a database and associated application software, referred to as the Registration of Persons (ROP) sub-system of ImmD's Processing Automation (PA) system;
- a microfilm archive, containing microfilm records of all applications, change requests and supporting documents.

The following sections examine each of these elements and their use.

The Card and Its Contents

Identity cards have been issued in Hong Kong since 1949. The content has changed over time, with both additions and deletions. Initially, the card displayed the thumbprint (removed in 1973); and, where applicable, the passport number (removed in 1983).

Most persons In Hong Kong are required to hold a card. The exemptions and exclusions, authorised under ROP Reg 25 and 25A, are:

- children under 11 (unless they need a HKSAR passport issued);
- travellers in transit;

[10] Statement by the Governor in the Legislative Council, 23 October 1980, Hong Kong Legislative Council Hansard, 1980, pp.103 to 106.
[11] Op cit, p.105.
[12] Op cit, p.106.

- persons permitted to remain In Hong Kong for less than 180 days;
- the aged, blind or infirm persons who can satisfy the Immigration Department that compliance with the Ordinance and the regulations to apply for the issue of a card would injure their health or the health of others; and
- Vietnam refugees pending resettlement elsewhere.

A number of categories of card exist, and the data held on the card, the database and the microfilm archive varies between these categories. The total number on issue is about 7.2 million, and about 500,000 are issued or re-issued each year. The primary categories are:

depending on the person's residence rights and current residence:

- **Permanent ID Card (PIC)**, for persons with right of abode (which has a green background, and bears a statement that the person has right of abode in Hong Kong). 6.5 million are on issue, and c. 400,000 are issued or re-issued each year;
- **ID Card (IC)**, for other persons resident in Hong Kong (which is readily distinguishable from the PIC because it has a pink background, and does not contain a statement about 'right of abode in Hong Kong'). About 700,000 are on issue, and about 130,000 are issued or re-issued each year;
- **Overseas Permanent ID Card (OPIC)** for persons with right of abode residing overseas and applying for the card in connection with the issue of a HKSAR passport (the card has the word 'ISSUED OVERSEAS' printed in red on the card face). About 22,000 are on issue, and about 500 are issued each year;
- **Consular Corps ID Card (CCIC)** for consuls, consular staff and their dependents (the card has a unique format). About 5,000 are on issue, and about 500 are issued or re-issued each year.

depending on the person's age:

- **Minor**, for persons under 11 years (only required if a HKSAR passport is requested). About 500,000 Minors PICs and 7,000 Minors OPICs are on issue, and about 25,000 Minors PICs and about 200 Minors OPICs are issued each year;
- **Juvenile**, for persons 11-17 years. About 650,000 Juvenile cards are on issue, and about 125,000 are issued or re-issued each year;
- **Adult**, for persons who have attained the age of 18. About 6 million Adult cards are on issue, and about 350-400,000 are issued or re-issued each year.

In this report, the term Hong Kong ID Card is used to refer generically to all of the above categories. (The term HKSAR ID Card is used in the report to refer generically to all the categories of identity card to be issued under the proposed new scheme).

The current card has been issued since 1987 and contains[13]:

- the card-number;

[13] Schedule 1 to the ROP Regulations governs the contents of an identity card.

- the person's name:
  - in English; and
  - where relevant, in Chinese script, with the equivalent Chinese Commercial Code (CCC);

(Under section 5 of the Registration of Persons Ordinance (Cap. 177) every person registered under the Ordinance is required to use the personal name and surname entered on his or her Hong Kong ID Card in all dealings with the Government. Aliases may, however, be recorded on the application and hence on the ROP database and the microfilm archive, but not on the card);

- the person's date of birth;
- the person's photograph (where the holder was 11 or older at the time of application, ie: not on Minors cards);
- codes, most commonly showing right of abode and eligibility for a re-entry permit; gender; whether the person's place of birth was Hong Kong, Mainland of China, Macau or other; whether particular changes have occurred (e.g. name or gender, date or place of birth); and whether a previous card was lost;
- the office and date of issue;
- the date of first registration.

The Contents of the ROP Database

The scheme is supported by a sub-system of ImmD's Processing Automation (PA) system, called the Registration of Persons (ROP) sub-system. The ROP sub-system performs the following functions:

- assists in the processing of applications for Hong Kong ID cards;
- maintains a database of data concerning ID cards;
- supports on-line enquiry services, in some cases around-the-clock; and
- enables data transfers within and beyond ImmD (see next paragraph); and
- security, controls, audit and management statistics.

The ROP sub-system relies upon common portions of the PA database, and has in addition some record-types which are ROP-specific.

The primary key of the Person File is the Person Reference Number (PRN). From the perspective of the data schema, the ID Card number is merely one of a number of retrieval keys. (Others include English Name, and Chinese Commercial Codes, which are a codified form of the ideogrammatic representation of each character of the holder’s Chinese name).

The PRN is a person-identifier used within all ImmD systems, and is assigned to all persons known by ImmD to be in Hong Kong, with the exception of those short-stay visitors who do not need visas, but including persons of interest such as illegal immigrants and over-stayers. It is generated under several circumstances, in particular:

- when a birth is registered;
- if an application for an ID card is received (whether or not it is approved and an ID card is issued);
- on application for visa; and
- when a person of interest becomes known to ImmD.

The ROP database is populated with some (but not all) of the data contained in the initial application for an ID card. The collection of this data is authorised by Regulation 4 of the Registration of Persons Regulations made pursuant to section 7 of the Registration of Persons Ordinance (Cap. 177).

The following data provided by the person on the application form is recorded on the ROP database:

- ID card number (if already assigned, e.g. for a Minor or Juvenile card)
- English name;
- Other Names in English, recorded as Aliases;
- Chinese Commercial Code (CCC) for the Chinese name;
- Date of Birth;
- Place of Birth;
- Sex;
- Travel Document Type (but not number);
- Nationality Claimed.

The following items that are provided by the person on the application form are not recorded on the ROP database:

- Travel Document Number, and its Place and Date of Issue;
- Profession/Occupation;
- Residential Address and Telephone Number;
- Name of School/Company and Telephone Number;
- Marital Status;
- Education Level;
- Spouse's Full Name and HK ID Card Number;
- Parent or Guardian ID Card Number (in the cases of Minors under 11 where relevant, and of Juveniles under 18).
- whether ordinarily resident in HKSAR for not less than 7 years;
- Signature and Date;
- Left Thumbprint (or of another thumb or finger);
- Photograph.

The ROP database contains, where applicable, additional information that is generated as part of application-processing activities. This includes:

- Application Reference Number and Nature Code;
- Application Status and Result Codes;
- Non-Routine Indicator;
- Current Residential Status;
- Right of Abode Status;
- Overseas Indicator;
- Date of Birth Verified Indicator;
- Acknowledgement of Application Details;
- ID Card Prefix, Number and Check-Digit;
- ID Card Registration Date;
- additional details re Consular Cards;
- fee payment details;
- Microfilm Index reference;
- ROP Office Details.

The ROP database contains, where applicable, additional information that is generated as part of the processing of applications and change of registered particulars, submitted by the person concerned. Examples are:

- Date-of-Birth Changed Indicator;
- Name Changed Indicator;
- ID Card Loss Count;
- Date of First Registration.

The ROP database contains, where applicable, additional information drawn from other sources. This includes:

- Juror Status;
- Deceased Indicator (resulting from a notice from the Deaths Registry, or directly from next-of-kin to ImmD);
- Overseas Indicator, known as the Registrant Status (resulting from the return of identity cards from residents who have left for good.

The ROP system draws on the PA common data area where needed, in particular data provided by the Registries of Births and Deaths and Application for Entry Visa. Birth Registry information may be consulted during the processing of the initial application for a card. Marriage Registry information appears to be consulted only in unusual circumstances, but is available to ROP staff. In the case of deaths, the Registry updates the Deceased Indicator to invalidate the card.

Information provided at the time of applying for an employment/dependent visa may also be referenced during the processing of the initial application for a card.

No person-to-person linkages exist between the entries for persons on the ROP database. In the case of a minor, the HK ID Card Number for the Guardian is recorded in the file, and application forms and Notification of Change forms contain spouse name and card number; but in neither case are any computerised linkages implemented.

Some linkages can, however, be inferred from the microfilm archives held by ImmD. In particular, because application forms contain spouse name and card number, 'family tree' data can be extracted by ROP's Confidential Registry, by a manual process, in order to satisfy requests for information from other sections, in particular the Right of Abode Section, and other agencies, in particular the Police.

The Contents of the Microfilm Archives

The microfilm archive contains microfilm records of:

- the application form, including:
  - the personal data (some of which is on the card and database as well, and some of which is on the database but not the card, but some of which is on neither);
  - the photograph (which is also on the card, but not on the database); and
  - the thumbprint (which is on neither the card nor the database);

- copies of all documents provided in support of the application, such as a travel document (i.e. passport), birth certificate, school handbooks with photo of the minor/juvenile , evidence of change of name and documents in support of an application for change of registered particulars; and
- paper index cards containing key ROP data and in use between 1960 and 1983.

The Circumstances of Application for, and Issue of, the Card

Pursuant to section 3 of the ROP Ordinance every person in Hong Kong is required to be registered under the Ordinance, unless exempted or excluded from the provisions of the ROP Ordinance. Regulation 25 of the ROP Regulations provides for those categories of persons who are exempted from registration and Regulation 25A provides for those who are excluded from registration.

Every person who needs to register, and to have a new or replacement card issued, must attend one of six ROP offices in the Hong Kong SAR. The physical traffic through ROP offices comprises persons who are new to the system, persons in transition from one card to another, and those whose card is lost or damaged. Card-holders notifying a change of registered particulars can do so without attending except where the change affects the content of the card and therefore requires a replacement.

Categories of persons who are new to the system include the following:

- persons aged under 11 who apply for a Minors ID card (which is necessary if they require an HKSAR passport). There are about 23,000 of these each year;
- persons who have reached 11 years of age who are required to acquire the Juvenile ID card, if they have never applied for a Minors ID card. There are about 26,000 of these each year;
- persons arriving in Hong Kong to live or work for longer than 180 days. There are about 115,000 of these each year;
- overseas applicants who apply for a HKSAR passport. There are about 500 of these each year.

Categories of persons who are in transition from one level of card to another include the following:

- persons who attain the age of 11, and who are then required to acquire the Juvenile ID card, and who already have a Minors ID card. There are about 61,000 of these each year;
- persons who attain the age of 18, and who are then required to acquire the Adult ID card. There are about 91,000 of these each year;
- persons whose rights have changed. There are about 45,000 of these each year. The reasons for issuing new ID cards to them include:
    - the acquisition of a right of abode in Hong Kong (IC to PIC);

- the loss of a right of abode, but the granting of a right to land in Hong Kong (PIC to IC);
- change in the residential status in Hong Kong e.g. from limited to unlimited stay (IC with changes to the codes); and
- a change in eligibility for a re-entry permit (PIC/IC with changes to the codes).

Categories of persons needing to have a replacement card issued include the following:

- persons who have lost their card (which accounts for about 500 of the daily 2,200 applications, or 130,000 each year);
- persons whose card has been damaged or defaced (which accounts for about 22,000 each year);
- persons required to register changes which affect the card content. These appear to be about 10,000 each year, and include:
  - name change (e.g. by deed poll, or by marriage - in which case the change is optional). It appears that the proportion of women who upon getting married formally advise change of name, or addition of their husband's name to their own is quite low;
  - date of birth change (due to new evidence);
  - change to personal data represented by codes;
  - place of birth;
  - gender.

The total number of persons processed per day is about 2,200, for about 270 days p.a., or about 0.5 million p.a. There are about 7.2 million valid cards on issue, with a resident population of about 6.8 million (including relevant persons living overseas); so the number of cards issued in any one year represents about 7% of the total pool of cards.

The Process of Application for the Card

Every person who needs to have a new or replacement card issued must attend one of six ROP offices in Hong Kong SAR. A telephone appointment system is available, which ensures getting a reservation even if there is high demand on the day. Having an appointment avoids the initial queue only. There are no special arrangements for VIPs or celebrities.

A substantial, multi-step procedure is involved, which requires about 90 minutes from entry to the office. The sequence of steps involved in the application process is as follows:

- queue for obtaining a tag;
- acquire an application form;
- fill in the application form;

- queue for the photograph taking;
- have a photograph taken;
- queue for the thumbprint operator;
- have a thumbprint taken;
- queue for the application assessment;
- have the application assessed, and submit the evidence required;
- await a call to the desk (during which time the information on the application form is checked against the database);
- present for interview (which, where a person's previous card is present, includes a check of the person's appearance against that photograph on the old card);
- await a further call (during which time the Acknowledgement of Application document is compiled, printed and prepared);
- present again at the desk to receive the Acknowledgement of Application, or, if payment is required (a person's initial card is free, but all losses and many kinds of amendments cost $HK395), await the call to the Shroff (cashier);
- receive the Acknowledgement of Application. This contains most of the data which will appear on the identity card, a copy of the photograph of the applicant and a digitised representation of the photograph. The Acknowledgement Form is usually valid for six weeks from the date of application.

The ROP Ordinance acknowledges that some of the aged, blind or infirm should not be required to go through the registration process, by providing exemptions from the need to hold an ID Card[14]. No allowance is made according to law for conscientious objection or other sensitivities in relation to acquisition of any of the photograph, thumbprint or personal data, except that persons without a complete thumbprint give a fingerprint instead. ImmD asserts that the need for the system to be comprehensive is overriding, and that this is generally accepted as both necessary and equitable.

In general, persons living or working overseas do not need to apply for a new or replacement ID Card until they return to the HKSAR. A different, qualified form of card can, however, be issued overseas, but generally only in connection with an application for a new HKSAR passport. In such cases these persons will have to attend one of the Chinese diplomatic and consular missions for the application and collection of cards.

Authentication Procedures

There is a succession of authentication procedures used during the application and issue processes. The primary procedures are:

- during the initial application process, an officer (application assessor) performs an initial check of the application form for completeness, the quality of photographs and thumbprints, and the availability of the required supporting

[14] ROP Regulation 25(e)

documentation, and approves the kind of card to be issued, appropriate to the person's immigration status;

- at a later point in the initial application process, another officer calls the person to an interview. Where there is an existing database entry, this includes checking against that data. That is followed by entry of relevant data into the database;
- a checker (any officer other than the one that performed the interview) then checks the data, prior to issue of the Acknowledgement of Application;
- after the application process has been completed and the Acknowledgement of Application issued (and after the applicant has left the office), a further officer checks the print quality of the data card;
- the applications are assembled into batches of up to 30 of a similar type.
    - For first-time cards, the data card is sent to the Government Printer and the application forms to the microfilm office;
    - In respect of replacement cards, after the initial application process, and during the period of card production, the Verification Officer checks the application form against the microfilm of the applicant's most recent application, placing particular weight on a visual comparison of the old and new thumbprints (with the standard required being five points of correspondence, rather than the twelve generally required for court evidence). He/she also takes into account the photograph, signature, and the personal data. The verification staff comprises about 10 uniformed officers. Discrepancies and inadequacies, and all instances of lost cards, require review by the duty officer. These may lead to a call for a replacement thumbprint, or referral to the Investigation Section.

Some of the data is subject to authentication, but some is self-reported without cross-checking, including claimed nationality, profession/occupation, residential address and telephone number, school/company address and telephone number, marital status, education level, and name and Hong Kong ID Card number of spouse.

The Process of Card Issue

The printed image from which the card will be manufactured is sent under secure arrangements to the Government Printer, from where the card is received back in the same manner, and held in secure storage.

The card is available to the cardholder 15 working days after the application has been successfully made and an Acknowledgement of Application issued.

Normally, the individual returns to the same office, and presents the Acknowledgement of Application at the relevant counter. Their appearance is checked against the photographs both on the Acknowledgement of Application and on the card, and they are given the card.

Alternatively, two proxy arrangements are available:

- the person may nominate a proxy at the time of application, by completing an authority form, including the proxy's name and ID card-number. When the proxy picks up the card, they present the Acknowledgement of Application, the authority form, and their ID card. These are checked for completeness and consistency, and the proxy is given the card; or
- the person may nominate a proxy at a later time. In this case, the proxy must also bring a further document bearing the proxy's signature. In addition to the normal controls, the signatures are compared.

The Production of Microfilm Records

The Verification Office sends the batches of applications and attachments, to the Microfilm Office. They are filmed, and a visual check of the quality of image is performed. The microfilm reference is added to computer database entry for each application.

Each microfilm record is assigned a roll film number. The microfilm reference/roll film number is then entered into the database and indexed to the persons database record using the PRN as the identifier to link up with the respective identity card. A person may have many microfilm references resulting from applications (irrespective of the result) and notifications over a long period of time. A microfilm reference may also be indexed to several PRNs (juvenile/guardian cases or collective notification of changes).

Four copies of each microfilm are made.

The paper applications are held for 4 months, and are then securely disposed of.

Security Measures

ROP procedures include many controls of various kinds. These have been refined in line with recommendations by ICAC to reduce corruption opportunities.

A wide range of security measures are deployed, including:

- checks on printing quality of the data card after the issue of the Acknowledgement of Application, but prior to the submission to the production unit;
- recording on the database that a card is now issued only when it has actually been handed to the individual or their proxy;
- controlled access to sensitive areas of ROP premises, particularly those containing microfilm; and
- punching a hole in, and then controlled disposal of, old cards.

Access control to the ROP sub-system is the same as that which applies to all ImmD systems. It applies to all locations from which access is possible; and it will apply to temporary sites such as the additional card-issue points envisaged for the issue of

the future HKSAR card. The security regime is sophisticated, and comprises the following elements:

- each person is issued with a personal user ID/password pair;
- in all cases, multiple sign-ons at the same time on two different devices are precluded;
- the user ID/password pair is invalidated during periods of absence, e.g. when on leave. However because the Human Resources system is not automated, it is not able to integrate directly with the access control system – manual procedures apply;
- associated with each user ID/password pair is a set of privileges that are maintained by a system controller. The privileges associated with a user ID/password pair are as follows:
    - they are primarily determined by the transaction-type, each of which provides access to and/or amendment capability in relation to a defined set of data-fields from a defined set of record-types;
    - control is also exercised over the locations in which the user ID/password pair can be used;
    - there is, however, no provision for individual records to be suppressed depending on any criterion such as the name, card-number pattern, or any special protection-code;
- all accesses and amendments are logged to an audit trail, including the user ID, time-stamp, the workstation-id and its location;
- the audit trails are subject to manual inspection, and procedures exist requiring acknowledgement by individual staff and checking both by security staff and by individual managers;
- however, no automated analysis for anomalies is currently undertaken (although analysis for at least one category of anomaly is being considered for the replacement system).

Despite the security measures, it is to be expected that some instances arise of identity impersonation and theft, card duplication and forgery. Statistics in relation to impersonation and card forgery, and in relation to the detection, and repatriation or prosecution of offenders for these offences handled by ImmD, are available.

The Processing of Notifications of Changes of Personal Data

Under ROP Regulation 18, persons are required to notify changes of registered personal data. This is done through the use of three forms:

- Application for Amendment of Registered Particulars (name, date of birth, place of birth, and other. The first two imply the need for a replacement card);
- Notification of Change of Address; and
- Notification of Change of Particulars (alias, nationality claimed, occupation, firm/school name and address, residential address, marital status, travel document number, dependent children's names and ID Card Numbers).

Although Regulation 19 specifies penalties for failure to notify changes the requirement is not routinely enforced. The notification forms contain a polite request for further changes to be notified, and no reference to it being a legal requirement.

The two Notification forms invite the person to request forwarding of the changes to the Registration and Electoral Office (REO) for updating the electoral roll and to the High Court for list of persons eligible for jury service.

Where a person has opted for one or more of these transfers, the address information will be passed to the organisation concerned in batches. In the case of REO, it is keyed into a floppy diskette provided by REO whereas for information to the Registrar of the High Court it is a manually prepared list.

The Circumstances of Use of the Card

Pursuant to section 17C of the Immigration Ordinance (Cap 115), all persons aged 15 and over who hold a HK Identity Card are required to carry proof of identity with them at all times. Proof of identity includes the Hong Kong ID Card and a valid travel document (section 17B of the Ordinance). In practice, people subject to the requirement generally carry their Hong Kong ID Card. Juveniles aged 11-14 are required to possess a card but are not required to carry it, and children younger than 11 who have a card (issued in connection with HKSAR passport) are not required to carry it. In addition, there are requirements to carry Hong Kong ID Cards in specific circumstances, e.g. frontier areas pursuant to an Order made under ROP Regulation 11.

There are various provisions to cater for circumstances in which a person who is required to hold a HK ID Card does not have one, including:

- pending application for registration;
- where they hold an Acknowledgement of Application (valid for six weeks but typically only held for 15 working days while awaiting card issue);
- where they have lost their card.

The formal uses of the card include:

- inspection by any immigration officer or immigration assistant, any police officer, or any person or member of a class of persons authorised by order published in the Gazette, who, in all cases, is in uniform or who produces his official documentary identification if required to do so (section 17C of the Immigration Ordinance); or any person authorized for the purpose by the Commissioner of Police pursuant to ROP Regulation 11(2);
- presentation when travelling into or out of the Hong Kong SAR, as an optional complement to a valid travel document for most of the IC holders, or as an alternative travel document for all PIC and some IC holders;
- presentation to an employer who is required to inspect the identity card of any person he intends to employ who is a holder of an identity card (section 17J of the Immigration Ordinance); and

- presentation to the ROP Sub-division of ImmD when applying for a replacement card (other than where the original has been lost or stolen).

Other government agencies routinely request presentation of the card for identity verification in support of the requirement that a person must use their registered name and card number whenever dealing with any government agency (ROP Ordinance, s.5).

Individuals are also commonly requested to present their card in a wide range of other circumstances, both by public and private sector bodies. There is no legal constraint on this, although there are limits on the keeping of copies and the recording of the Identity card number (see below). While there is no legal requirement to comply with such request unless it is made pursuant to section 17C of the Immigration Ordinance, the requesting party can decline to provide the service or benefit concerned unless the ID card is presented, and this has the effect of making the presentation of the card necessary in practice in many circumstances.

The Process of Use of the Card

In some circumstances, the card may be merely inspected by the person it is produced to. This may or may not involve comparison of the person's appearance with the photograph. (Given that the photograph was taken on the most recent occasion of re-issue of the card, i.e. at age 18, or any subsequent change of card data, there may be considerable differences between the two). Inspection by government agencies may also include questions, the answer to which is apparent to the questioner from the appearance of the card (in particular the set of codes that appears on its face).

In some circumstances, the number of the card may be used by the person it is produced in order to acquire additional data that is stored in the ROP database or in the ImmD microfilm records (see below).

The Card Number and the Circumstances of Its Use

The Hong Kong ID Card number comprises:

- an alphabetic prefix. For example, the prefix W indicates an 'imported worker' or a ‘foreign domestic helper’. Until 1983, each office that issued cards had a block of prefixes issued to it (e.g. Hong Kong Island A, D; Kowloon B, E, G; and New Territories C); hence remaining old card-numbers contain a limited amount of meaningful information;
- a six-digit number, which is assigned sequentially within blocks; and
- a check-digit, shown on the card inside brackets.

In the case of persons born in Hong Kong since 1980, applicants applying for birth registration will be issued a birth entry number which will become his/her future identity card number, and is printed on the Birth Certificate. The number is assigned from the individual registry location’s own block of codes. Since 1995, this has been done under software control.

In the case of persons who were born outside Hong Kong, the ID card number is generated by the computer when they apply for an ID card. It is assigned under software control from a single block of numbers.

There is a wide range of formal uses of the card-number. These include:

- a requirement to furnish the number to any public officer in all dealings with government, both in respect of a person's own number and that of any other person whose particulars they may be required to furnish. The authority is ROP Ordinance s.5;
- the driving licence displays the holder's ID Card Number, and is therefore available to, and at least to some extent used by, all organizations that require or request production of the licence;
- the Inland Revenue Department (IRD) uses the number as its primary taxpayer Identifier;
- employers are required to keep a record of the names and, where permanent identity cards are held, the ID Card numbers of all employees (Immigration Ordinance s.17K); and
- the Police's ECACCS system uses the card-number as the primary key for identity authentication.

A wide range of other uses of the card-number have arisen, within and beyond government. Since 1998, these uses have been recognised by the Code of Practice on the Identity Card Number and other Personal Identifiers, issued by the Privacy Commissioner for Personal Data under s.12(8) of the Personal Data (Privacy) Ordinance. They include:

- where the use of the ID card number is necessary for any of the purposes mentioned in s.57(1) of the Personal Data (Privacy) Ordinance (safeguarding security, defence or international relations in respect of Hong Kong) or s.58(1) (prevention or detection of crime; apprehension, prosecution or detention of offenders; assessment or collection of any tax or duty etc);
- where the use of the ID card number is necessary for the exercise of a judicial or quasi-judicial function by the data user;
- to enable the present or future correct identification of, or correct attribution of personal data to, the holder of the identity card, where such identification or attribution is or will be necessary:
    - for the advancement of the interest of the holder (eg by a doctor to link medical records);
    - for the prevention of detriment to any person other than the data user;
    - to safeguard against damage or loss on the part of the data user which is more than trivial in the circumstances (eg by a driver in a motor accident);
    - to support legal documentation (eg on a contract);
    - in support of access control (eg in visitors books);

- as a condition of giving the holder custody or control of a valuable asset (eg car rental).

While these purposes, set out in the Code of Practice, are not legally binding constraints in themselves, they are the Privacy Commissioner's view of how compliance with the Data Protection Principle 1 (Collection Limitation) applies to the ID card number, and will be taken into account in any proceedings under the Personal Data (Privacy) Ordinance.

The Code goes on to specify circumstances in which the HK ID Card Number may be used (Guidance on Compliance with Data Protection Principle 3 (Use limitation)). These include:

- for the purpose for which it was collected;
- in carrying out a matching procedure permitted under s.30 of the PDP Ordinance;
- for linking, retrieving or otherwise processing records held by [the data user], or by two or more data users for a shared purpose;
- for a purpose required or permitted by any other code of practice under the PDPO ;
- for a purpose for which the holder of the identity card has given his prescribed consent.

The Code also details the circumstances in which the card can be copied. These are broadly consistent with the permitted purposes of collection and use, except that the copying has to be necessary (eg: some uses such as visitors books will not justify copying).

It is clear from the Code that there are few constraints on the way in which even private sector data users can use the ID Card Number. Most uses would fit within one or other of the permitted circumstances. The main objective of the Code is to limit the gratuitous and wholly unnecessary dissemination of the number, e.g. by displaying it on badges or private identity cards, or publishing it; and to rule out its use in certain specific ways such as matching for marketing.

The Circumstances of Use of, and Disclosure from, the Microfilm Archive

Many uses of the microfilm archive are made within ImmD. These include:

- checking of applications, by ImmD's Verification Office, using their own copy of microfilm archives;
- urgent ImmD control-point requests for information, handled by ImmD's Immigration Telephone Enquiries Unit (ITEU). Requests are initiated by officers at control points in handling cases where returning residents have lost their identity card and have no other travel document in hand, by telephone 24 hours per day, directly to ITEU. Relevant microfilm records are extracted, printed and faxed, using dedicated machines. Of the order of 60-80 requests are handled each day, generating an average of 2-3 pages of fax. Turnaround time averages 8 minutes;
- urgent police requests for information, handled by ImmD's Immigration Telephone Enquiries Unit (ITEU). Urgent police requests for authentication are initiated by policemen on the beat, at any time of day or night. In response to these, relevant

microfilm records are extracted, printed and faxed, using dedicated machines with encryption facilities. Of the order of 15-25 requests are handled each day, generating an average of 2-3 pages of fax. Turnaround time averages 8 minutes. A signed request from the authorised police officer has to follow. This is usually received 1-2 days later. If it is not received, it is followed up;

- other semi-urgent requests for information, handled by ROP Microfilm Records Office. Requests are initiated by ROP's six registration offices, where a person presents without sufficient documentary evidence to constitute 'proof of identity' in relation to an application or an identity card to replace one which was lost, by telephone during office hours. Relevant microfilm records are extracted, printed and faxed, using dedicated machines with encryption facilities. Of the order of 20-30 requests are handled each day, generating an average of 2-3 pages of fax. Turnaround time averages 8 minutes;

- non-urgent requests from authorised agencies. Non-urgent requests are submitted in writing to the Confidential Registry. The requests are required to cite the relevant exemption under the Personal Data (Privacy) Ordinance (PDPO) (ss.57-58), and must be signed by specific authorised officers whose signatures are on file (and which are compared to file copies if they are not recognized). Approximately 100 of these are received each day, and there is a 2-4 week turnaround. Police use a proforma, but other requests are commonly in the form of a letter. Where requests do not comply with the requirements, the agency is advised. Many requests are for specific data, such as the address; but in some cases, especially from the police, the request is for all data. The police are also making an increasing number of requests for records of unspecified family members, pursuant to a specific permission from the Chief Secretary or delegate under ROP Regulation 24. The response usually comprises an extract, but sometimes the actual copy of the microfilm printout is provided, e.g. for evidentiary purposes;

- non-urgent requests from other outside organisations. Non-urgent requests are submitted in writing to the Confidential Registry and are the subject of individual case by case permissions under ROP Regulation 24. Most of these requests are related to legal cases or prosecution matters. For example, the Mass Transit Railway Corporation (MTRC) and Kowloon Canton Railway Corporation (KCRC) have been authorised in particular cases to obtain the address information for persons in breach of the MTRC/KCRC by-laws;

- requests by individual card-holders, for provision to various organisations. Compliance with requests by the holder of a Hong Kong ID Card for a certificate of registered particulars is authorised under ROP Regulation 23. Only the holder themselves (or the parent/guardian who submitted the application on behalf of the applicant at the time of registration) may make such a request. Approximately 50 of these are processed per day by the Certificate Unit[15], and there is a standard 25-working day turnaround, although a shorter time may be available in response to an urgent request. The application must be accompanied by two photographs and must be submitted in person with

[15] Approximately 13,500 a year – no breakdown is available of the type of request, ie: the different reason given on the application form

production of the HKID Card for verification of the applicant's true identity. The information is extracted from microfilm, and inserted into standard template letters, designed for different purposes, and including one of the photographs. On receipt of the letter, the individual concerned can, where applicable, then provide the certificate to the organization that has asked them for it. Instances in which this arrangement is used are identified on application form ROP 122, and include:

- applications for migration to other countries;
- certification of aliases;
- proof of a prior declaration of marital status (required under certain circumstances by mainland authorities); and
- evidence of the relationship between a prior and a current identity, in relation to property ownership matters.

The Circumstances of Use of, and Disclosure from, the ROP Database

Internal uses of the ROP database include the following:

- on-line access by ROP's processing sections, including its six Registration Offices, Verification Office, Microfilm Records Office, and Overseas PIC Unit;
- on-line access by ROP's Confidential Registry and Certificate Unit;
- to ImmD's Immigration Control Automated System (ICAS), data concerning invalidated and lost cards;
- on-line access by ImmD's Immigration Telephone Enquiries Unit (ITEU), as part of the service to its control points (see section above on uses of the microfilm archive);
- on-line access by senior officers at control points in verifying identity cards;
- on-line access by senior staff of Investigation Division in investigations and authentication of identity card records received through the enquiry hotline; and
- assessment of various applications received by ImmD e.g. application for Right of Abode, passport, entry visas and extension of stay, etc.

External disclosures from the ROP database include the following:

- to the Hong Kong Police ECACCS system, online, around the clock. At the request of police in the field, a Police Communication Officer at an authorised location inputs the card-number and the date of issue, and receives an indication as to whether or not the card is currently valid by means of pre-defined codes. Access is only by designated officers in control centres. ECACCS is to be replaced by 2004 with a new system. The proposed new system is intended to be functionally equivalent, except for replacement of fax by electronic delivery, and enabling electronic signatures for requests (as part of a parallel government wide initiative);
- to the Police, via ImmD's Immigration Telephone Enquiries Unit (ITEU) (see section above on uses of the microfilm archive);

- to a wide range of agencies for a variety of purposes via ROP's Confidential Registry Unit (see section above on uses of the microfilm archive);
- to employers, via ImmD's Investigations Division, which operates a hotline to assist employers to ascertain whether an applicant has appropriate status to enable them to be employed, or are suspicious about card-validity. An employer provides to the hotline his own information and the person's name, ID card number and all other data appearing on the face of the identity card, and receives confirmation of card validity and the person's employability or otherwise. As it is a legal requirement for the employers to inspect documents of a new employee (s.17J, immigration Ordinance) and it is an offence to employ a person who is not lawfully employable (s.17I, Immigration Ordinance), the confirmation of identity card information is regarded as a measure in the prevention of crime for the purposes of the Personal Data (Privacy) Ordinance (s.58);
- to the Registration and Electoral Office (REO), which receives in monthly batches, on disk, changes of address of persons who have notified ImmD. This information is provided to the REO pursuant to the consent of the identity card holders and the requirements under various Regulations made under the Electoral Affairs Commission Ordinance (Cap. 541), e.g. paragraph 6 of the Electoral Affairs Commission (Registration of Electors)(Legislative Council Geographical Constituencies)(District Council Constituencies) Regulation. The notice printed on the back of application/notification form states that one of the purposes of collection is to provide necessary information to the REO to update the electoral roll. In practice this is only done for those individuals who have opted for this disclosure on the form. The list is specially compiled (keyed into a disk) for REO as ImmD do not have such address data in the computer system. The REO uses this data to re-assign voters to geographical constituencies, and notifies them accordingly. (Consent for this data matching procedure has been given by the Privacy Commissioner for Personal Data). The REO also provides ImmD periodically with a tape containing a list of ID Card Numbers of persons applying for electoral enrolment, and receives in return on disk name, sex, date of birth and right of abode status of the person (but not addresses) (A separate approval for this data matching procedure has been issued by the Privacy Commissioner for Personal Data). The furnishing of this information by ImmD is done pursuant to the requirements referred to above. There are corresponding ROP Regulation 24 permissions for these disclosures to the REO;
- to the High Court's Jury Office, via ROP's Jury Unit, in relation to jury status and personal particulars. It is an obligation for a qualified resident to serve as juror in the proceedings in the court. The Registrar of the High Court or the Commissioner of ROP is empowered under section 4A of the Jury Ordinance to ask for information with a view to compiling the juror list. Under s.4A, Universities are requested by the ROP Sub-Division to provide name, identity card number and address of graduates and ROP sends a letter and notification forms to ask the graduates to provide further information. The ROP Jury Unit informs the Registrar of the High Court of any individual who becomes eligible for jury service, either as a result of changes in particulars or by registering for the first time, and updates the ROP database by setting a flag. The flag is removed on receipt of notice from the High Court that a person no longer has juror status.
- to the holder of an identity card, in the form of Certificates provided by the Certificates Unit, (see section above on uses of the microfilm archive);

The legal authority for disclosures is outlined more fully in the Legal Analysis section in Part IV.

Access by Persons to Personal Data Concerning Themselves

The data on the ID card is visible. No data is stored in obscured form (such as embedded within the ID card-number, a bar-code or a magnetic-stripe), other than that in a set of codes displayed on the card-face. An explanation of the codes is publicly available.

Data on the ROP database and information on the microfilm archive is accessible to individuals, under the ROP Ordinance (Regulation 23) and the PDP Ordinance (Data Protection Principle 6 and section 18). The PDPO provides for exemptions from the right of access (ss.57-61). Access procedures are specified in Immigration Department Notice 338/99. IDN 338/99 suggests that in respect of ROP data and microfilm records the Certificate of Registered Particulars processes, (and fee of $395) apply. All requests for ROP data by the data subject him- or her-self would appear to be directed to that channel. About 13,500 requests for registered particulars are received per year although no breakdown is available to show what proportion of these are requests motivated solely by the subject's own interest, as opposed to requests made at the behest of third parties.

Underlying Infrastructure

Pre-production processes for cards are performed by ImmD, but the card manufacture is outsourced. Under the new system, card manufacture may be moved back in-house.

All microfilm operations are performed in-house and this will continue until the operation is phased out, which is currently scheduled for c. 2003.

The computer-based PA/ROP sub-system and database is a 1995 enhancement within ImmD's Processing Automation (PA) system. The underlying PA system is a 1992-94 development, incorporating some elements dating back to the early 1980s. The design and development of the existing PA/ROP software and database was performed by ITSD.

All current computing and networking resources are managed by ITSD staff, but within ImmD premises.

Special Arrangements

In any population, various categories of persons-at-risk exist, including some public officials such as judges, some VIPs and celebrities, victims of domestic violence or stalkers, ex-associates of criminals, protected witnesses, undercover operatives etc. Some jurisdictions make special provisions for suppression of details or specially restricted access to official records which might be used to locate or otherwise adversely affect such persons. In Hong Kong, there are generally no such special

provisions, although procedures are in place to ensure the safety of protected witnesses. Knowledge of these arrangements is intentionally restricted to a very small number of officers, as a security measure. Some other categories of persons at risk have the option of changing their name by deed poll and applying for a new ID Card. ImmD asserts that there is a general acceptance that there should be no other special arrangements, on equity and non-discrimination grounds.

PART III THE HKSAR ID CARD PROJECT

Context & History

The current HK ID Card scheme is to be replaced, for the following primary reasons:

- the current card is increasingly subject to forgery, and is to be replaced by a new form of card embodying new technologies that are more resistant to fraud;
- authentication of the cardholder's identity in the field needs to be improved because the present approach, based on the facial portrait reproduced on the card, lacks the desired level of accuracy;
- the technologies used within ImmD to support management of the data underpinning the card's integrity are obsolescent, and support will be withdrawn by the IT providers in the near future; and
- considerable improvements in the efficiency of ROP's operations are feasible, through the application of modern technologies to the work of the Registration, Records and Verification Offices.

It is intended that the new scheme facilitate some future enhancements to and extensions of ImmD systems, in particular the intended Automated Passenger Clearance system at control points.

The need for a new card was identified during a comprehensive review of the Immigration Department's Information Systems Strategy (ISS) in 1999. A project team was set up in October 1999 under a Deputy Director, and consultants were engaged to undertake a feasibility study. The study came to public notice in the context of seeking approval from the Legislative Council (LegCo) Establishment Sub-Committee for the Deputy Director position. A paper for the meeting of the sub-committee on 23 February explained the project. The paper acknowledged the sensitivity of the HKSAR ID Card Project as well as its complexity and scale. Members of the sub-committee expressed varying degrees of support for the project, with some having significant reservations and concerns about the privacy and confidentiality implications. In response to these concerns, the Administration agreed that the relevant LegCo panels should be briefed on the project before Finance Committee made any decisions. The concerns expressed by some legislators were reported in both the English and Chinese language press.

A paper about the feasibility study was prepared by the Security Bureau and presented to the LegCo Security Panel in March. This paper explained that while the main focus of the study was on ImmD's core businesses, the consultants had also been asked to consider the potential for other applications, including specifically voter registration, but more generally other value-added applications if a smart card option is chosen. The sensitivity of this in privacy and security terms was recognized and the consultants asked to given technical advice on addressing these concerns. Minutes of the Panel meeting indicate that some legislators were critical of proceeding with the new card before its contents have been decided, and sought assurances that the amount of information, and its uses, should be minimized. The

HK Human Rights Monitor was reported as wanting restrictions on what information on the card could be accessed by any one government agency.

Also in March, ImmD briefed the Privacy Commissioner for Personal Data (PCPD) on the project. The Commissioner wrote to ImmD on 15 March (see Appendix 2) expressing some significant concerns and recommending that a Privacy Impact Assessment be conducted in the planning stage, and offering to provide further advice when the Feasibility Study was completed. The Commissioner warned in particular about the risk of 'function creep' whereby data come to be used for additional purposes. Even where justified, he argued, *"… the net effect is an undeniable move towards an increasingly surveillance-prone society."* The Commissioner did however conclude by saying *"I firmly believe that with the right objectives, design, security and community education the Government will be able to implement a new ID Card system for the benefits of our community while at the same time safeguarding the right to privacy of our citizens."* The Commissioner's reservations about the proposal were quoted in press reports, which emphasized his desire for additional applications to be optional, and his concerns that a concentration of data on the card could assist identity theft.

ImmD received a market research report on the available technologies in April, and a two volume final report of the Feasibility Study in June.[16] The report correctly identified the need to comply with the Personal Data (Privacy) Ordinance[17], although it focuses mainly on the security, data quality and integrity aspects. There is some recognition of less tangible privacy issues in the Management Summary in Part One.

On 1 June, the LegCo Security Panel considered a further paper on the project. This progress report briefed the Panel on the main recommendations of the Feasibility Study. This included a section on Data Privacy and Security, with a number of recommendations, which are set out in Appendix 3. The final recommendation was for the engagement of specialist privacy consultants to undertake a Privacy Impact Assessment. Minutes of the Panel meeting are not yet available, but the press reports again reported legislators' concerns about the additional powers that the new card could give government over individuals. Both in March and June, some legislators linked their concerns about the new card to fears about the proposed legislation to enact article 23 of the Basic Law prohibiting treason, secession etc.. Reports also pointed out that PRC functionaries in Hong Kong are not subject to the Personal Data (Privacy) Ordinance. The Deputy Secretary for Security was reported as giving assurances that personal data such as medical records would only be stored on the card with the holder's consent.

In July, the ImmD project team briefed the Privacy Commissioner and his Standing Committee on Technological Development on the Feasibility Study Report (although it is understood that the PCPD has not been given a copy of the Report. In a letter dated 28 July, the PCPD confirmed the views of his Committee, expressed in the briefing meeting (Appendix 2). These include "serious reservations with regard to the potential privacy invasion in the use of the new ID Card, other than for ImmD purposes, by other government departments and the private sector." In light of clear evidence of privacy concerns amongst the HK population, the Commissioner's

[16] SITA (consultants) Feasibility Study on the HKSAR Identity Card System, June 2000: Part 1 - Management Summary; Part 2 - Technical Specification.
[17] in Part One s.7.6; Part 2 s.20.2.4

Committee called for wider public consultation than just through LegCo panels, and citizens to be given a discretionary choice, genuine and non-discriminatory, about applications about the new card other than its use for identification.

The project timetable will require that a firm proposal be put to relevant LegCo Panels, and then to the Finance Committee, before the end of 2000.

The proposed new system

The objectives of the scheme[18] are:
(a) to support and control the issue of HKSAR ID cards;
(b) to enable the issue of highly secure and technologically advanced HKSAR ID cards which will help to combat illegal immigration and also support ImmD core business, e.g. facilitation of automated passenger clearance;
(c) to enhance the efficiency and effectiveness of the ROP record keeping and retrieval system of the ImmD as well as the ID card registration and production processes through the application of new technologies;
(d) to facilitate the processing of all ROP business applications through interface with the existing computer systems of the ImmD; and
(e) to support an ID card replacement exercise for the whole of the HKSAR.

Salient Differences Between the Existing and Proposed Schemes

The most important differences between the existing and new schemes are as follows:

- the card:
  - a contact smartcard is to be used;
  - the card is to include a chip;
  - the chip is to contain machine-readable data, comprising:
    - names, sex and date of birth;
    - ID card number;
    - date of registration and/or issue;
    - the symbols relating to residential status;
    - current condition of stay (COS) and limitation of stay (LOS);
    - a digital image of the photograph (possibly compressed);
    - digital images of both thumbprints (converted into a ‘template’ using a one-way hash algorithm);
  - provided that a sufficiently capable 'upper-end' card is used, the chip may contain further machine-readable data, comprising:
    - one or more private digital-signature keys, protected by one or more PINs or other security mechanisms;
    - possibly one or more private encryption keys, protected by one or more PINs or other security mechanisms;

[18] From Feasibility Study Report Part I, p.9

  - one or more digital certificates associated with each key-pair;
- the data is to be able to be read by devices in a variety of locations;
- the visible data on the card will decrease (in particular, the connotation of sex-change embodied in the symbol 'B' may be removed);
- it is not presently intended that any bar-code or other data-representations be used;

- card-receiving devices:
  - fixed-location terminals are to interact with the cards;
  - mobile, possibly hand-held, terminals may also be deployed;
- the card-number:
  - it appears that there is to be no change, other than its storage on the chip in machine-readable form in addition to its appearance on the face of the card;
- procedures within the ROP:
  - modern data and image capture and display technologies are to be applied, supported by workflow management, and card production will be brought in-house;
- the ROP database and system:
  - these are to contain additional data-items and associated processes and procedures, most significantly:
    - a digital image of the left thumbprint (previously collected on hard-copy application forms, and stored on microfilm only);
    - a digital image of the right thumbprint (which has never previously been collected or stored);
    - a digital image of the photograph (previously taken during registration and attached to hard-copy application forms, and stored on microfilm only, except for the digitised image printed on the temporary Acknowledgement of Application);
    - the address information, in addition to the digital image of the application form, will be temporarily stored as a separate image before transfer to REO. After that, the address will only be stored as an integrated part of the application image. (previously collected on hard-copy application forms, and stored on microfilm only. At present, such changes of address information are typed and tabulated by using a standalone personal computer and stored on a diskette for transfer to the REO);
    - a digital image of each document that is currently microfilmed. This data will not be converted into machine-readable text by optical character recognition (OCR), although this will remain a possibility just as the current microfilm records could be scanned and converted with OCR;
- the microfilm archives:
  - these are to be converted into digital form;

- once the new scheme is in operation, the microfilm production is to cease, because all documents would be captured in image-form; all inquires to microfilm will cease after the completion of the conversion exercise.

• the uses of the card scheme;

In addition to being the replacement ID card, to be used in all the circumstances that the existing card is used, it is intended that the card be used for further ImmD purposes, in particular:

- Automated Passenger Clearance;
- possible building and location access control for ImmD staff (through additional functions loaded onto the HKSAR ID Cards of ImmD officers and other employees; (This additional function was proposed by the FS consultants but ImmD has no plan to implement it.)

ImmD asserts that there is no current intention to use the HKSAR ID Card for any other purposes and that any additional uses would require legislative changes. There is a separate process, being co-ordinated by the Information Technology and Broadcasting Bureau (ITBB), looking at potential applications for a multi-application smart card, which may recommend adding functions to the HKSAR ID Card.

Examples of new uses by other government agencies, which have been mentioned as at least possibly under consideration by the ITBB steering committee, are:

- as a replacement for the existing driver's licence, which already carries the ID Card number;
- as a library card;
- as a health card, including storing some medical records;
- for electronic voting;
- for digitally signing messages to government agencies;
- as a senior citizen concession card (although a new non-smart card was introduced in September 2000).

It is possible that increased use may be made of the new card by other governments as a complement to a passport or other document**.** ImmD has however already resisted suggestions that the HKSAR ID Card should conform to an ICAO recommendation for particular standard of machine readability.

The Feasibility Study report speculated about other potential uses by non-government organizations, including businesses:

- as a health card;
- as a debit/credit card;
- for ticketing.

Both government agencies and non-government organizations could also be interested in the use of the card as a stored value 'e-purse' to make payments, including as part of government electronic service delivery (ESD) initiatives.

The following sections discuss the proposed or likely changes in more detail.

The Contents of the Card

The content of the card is not yet fully determined, but the current technical specification is fairly detailed.

It appears that the personal data visible on the face of the card may be subject to little or no change. Possible changes include (in particular, see Part II, p.225):

- continued printing of at least ID Card Number and Issue Date in OCR-readable font;
- removal of the DOB Verified indicator (removed entirely);
- removal of Issuing Office / Collection Office Code (removed entirely);
- possibly, removal of the asterisk symbol (denoting eligibility for HK re-entry permit) (removed entirely);
- removal of Previous Card Lost Count (removed entirely)
- redefinition of Symbol 'B', to remove the connotation of sex change.

A fundamental requirement is that the card store data internally in the chip, in a secure manner, and in some cases in updateable form. The data to be stored on the chip would appear likely to include the following:

- the data-items that currently appear on the face of the card (subject to the qualifications in the previous paragraphs);
- additional data items, in particular:
  - a digitised photograph or compressed version of the image, which can be used by the chip and/or a processor in a terminal or connected server, to display the image on a screen. The image will be subject to security precautions in the form of compression, or encryption. A JPEG image would require of the order of 2-4KB of storage space;
  - a 'template' of the left thumbprint, which can be used by the chip and/or a processor in a terminal or connected server to compare with a newly captured thumbprint. The image will be subject to security precautions in the form of one-way hashing and encryption. Such a 'template' may require 0.5-2KB of storage space;
  - the template of the right thumbprint, as a fallback or further authentication feature, to be stored in the same manner as the left thumbprint, and requiring the same storage space again;
- on ID cards other than Permanent Identity Cards (PICs):
  - condition of stay (COS), which may be changed without necessarily requiring re-issue of the card; and
  - limit of stay (LOS), which may also be changed without necessarily requiring re-issue of the card.

There is no intention to store data in any other form on the card, such as:

- in a bar-code. (The possibility of installing bar-code scanners is mentioned in Part II p.60; but this only refers to the bar-codes on application forms); or

- on a magnetic-stripe.

Because card-products change quickly, it is likely that the cards issued in bulk at the commencement of the new scheme would be no longer available a short time later (perhaps as long as 2 years or as short as 6 months**).** Although the card-size and contact specifications have been stable for some time, ImmD will need to handle multiple card products concurrently and to set this compatibility requirement when placing orders. There is however no guarantee that later card-products will be backward-compatible.

Generic Functions of the Card

The functions that the card is to perform are not yet fully determined. They may include the following, dependent on technical feasibility, policy decisions and costs:

- a fundamental requirement is that the card participate in two-way authentication processes, to ensure the integrity of processes. The functions involved are:
  - the card needs to respond to challenges issued by terminals, in order to authenticate itself to the terminal as a valid card (and possibly also to provide some technical information about the card-type);
  - the card needs to issue challenges to terminals and validate the responses, in order to authenticate the terminal (and possibly also to gather some technical information about the terminal-type)
  - the card needs to validate requests from terminals, in order to authenticate the circumstances in which data is disclosed, and in which it is updated;
- comparison of data from cards with data from card-receiving devices, such as a thumbprint-reader/digitiser or secure PIN-pad;
- if the scheme is to support additional applications beyond the updated equivalent of the current HK ID card's functions (together with the additional ImmD functions), including such possibilities as digital signatures and electronic cash, whether they are operated by ImmD or by other organizations:
  - application zones or regions on the card, that are protected from one another by layers of hardware, operating system and application protections, to ensure a very high degree of application and data integrity;
  - separation of 'what you know' (e.g. PIN) or ‘what you are’ (biometric) authentication of the user, for each application;
- means to capture and amend PINs;
- if the scheme is to support digital signatures, whether in conjunction with additional ImmD applications, or for additional applications used by other organisations:
  - key-generation, of keys of sufficient length to be secure during the life of the card, performed in a manner that is certifiably secure;
  - key-storage, in a manner that is certifiably secure, and will not, under any circumstances permit disclosure or discovery of the key; and

  - preclusion of the use of the digital-signature private key, without effective 'what you know' (e.g. PIN) or ‘what you are’ (biometric) authentication of the user;

- if the scheme is to support asymmetric encryption of messages, whether in conjunction with additional ImmD applications, or additional applications used by other organisations, similar features are needed as for digital signatures;
- means of upgrading card functions, including application features in general, and security features in particular.

Generic Functions of Card-Receiving Devices

Card-receiving devices are to be installed, which may be fixed-location and/or mobile/hand-held, which are to be able to interact with the chip on the card. The kinds of terminals and the functions that they are to perform have not yet been fully determined. They may include the following generic functions, dependent on technical feasibility, policy decisions and costs:

- a security access module (SAM), to ensure that the ID card application has very high levels of application and data integrity against external threats;
- participation in two-way authentication processes with cards;
- acquisition of data from cards;
- secure acquisition of thumbprint, and either provision to the card, or performance of comparison within the card-receiving device. Comparisons have to be performed between a thumbprint live captured by the device and one acquired from some other source (in particular from the card's storage area). This has to be performed in such a manner that there is no risk of spoof attacks of fingerprint image. The capability exists to compare the newly-captured print with that in the ROP database, but it is not currently envisaged that this would be done;
- comparison of data from cards with data from devices attached to or forming part of the card-receiving device, such as a thumbprint-reader/digitiser or secure PIN-pad;
- submission to cards of requests for update of card-data, including validation of the card's response;
- if the card-receiving device is to support additional applications beyond the updated equivalent of the current HK ID card's functions (together with the additional ImmD functions),:
  - multiple separate security access modules (SAMs), to ensure very high levels of application and data integrity against both external threats and other applications on the card;
  - acquisition of PINs by means of a secure PIN-pad as for ATMs and EFT/POS terminals, such that the PIN is never capturable;
- if the scheme is to support digital signatures:
  - secure PIN-processing, in order to provide 'what you know' authentication of the user, prior to permitting use of the digital signature private key.

Card-receiving devices will need to be able to cope with multiple card-products, because of their short period of availability. This might involve the need for multiple SAMs each designed to interact with a different version of the card.

Applications of the Card and Card-Receiving Devices

A variety of applications are envisaged. The following are the most apparent:

- some card-receiving devices will perform comparison between the stored and the newly-measured thumbprint, in order to authenticate the person's implied claim that the card presented is their own. The primary contexts in which this function may be performed include:
  - commencing in the short term, at fixed ROP Registration Offices, plus a mobile team for remote areas (e.g. outlying islands);
  - possibly in the short term, by standalone, unsupervised kiosks (enabling cardholders to check the contents of their cards);
  - in the short-to-medium term, by policemen on the beat;
  - in the medium term, by ImmD staff at control points as part of the intended Automated Passenger Clearance system (in which case those devices may in time still be staff-supervised but with minimum supervision);
  - possibly in the long term, by standalone, unsupervised kiosks (enabling cardholders to submit notification of changed particulars);
- some card-receiving devices will display the condition and limitations of stay (COS and LOS):
  - to ImmD officers in the Investigation Division;
  - possibly to police on the beat, thereby enabling them to recognise and deal with cases of apparent overstay or breach of condition.
- Some card-receiving devices might also be used to authenticate the person's claim that the card presented is their own, and to enable the use of the private digital-signature key, also by fingerprint comparison, e.g.
  - in the medium term, as a means of signing electronic messages to government agencies;
  - in the long term, as a means of signing electronic messages to other organisations;
- at least some of the card-receiving devices would be able to update some or all of the data on the card, e.g.:
  - ROP Registration Office devices would have the capability to amend the COS and LOS only;
  - devices in P&V offices might be able to update COS and LOS;
  - devices at ImmD control-points might be able to update COS and LOS;
  - for data integrity purpose, no other device to update any ImmD/ROP data item is intended.
- Other applications of card-receiving devices are mentioned in the Feasibility Study Report but ImmD asserts that there is no current intention to implement

them. They include use of card-receivers to authenticate the person's implied claim that the card presented is their own**,** again by finger print comparison, in additional contexts, e.g.:

- for access control to government and other buildings;
- as a means of achieving login to government or other computer systems.

The Contents of the ROP Database

It is envisaged that the ROP Database contents will differ from the current scheme in the following ways:

- digital image of the photograph, compressed and/or encrypted;
- digital image of the left thumbprint, compressed and/or encrypted,;
- digital image of the right thumbprint, compressed and/or encrypted,;
- an image of each document provided by the person concerned, including application forms, supporting documents, and notifications of change of particulars;
- address will not be stored as a data item nor in a separate image record. The address information will be scanned as an integrated part of the document image and stored permanently. The address information will, however, be highlighted and stored temporarily after the scanning process of application/notification forms and be passed to REO in a collective manner as a batch backroom job. There is no intention of converting the scanned image of the address into machine-readable (e.g. ASCII) text.

The condition of stay (COS) and limit of stay (LOS) are to be added to the identity card during the personalisation process. Data are not stored in ROP database. They are to be obtained from the P&V (Permits and Visas) system.

In addition, a new log of enquiries made to persons' image record is to be maintained within the ROP sub-system. This is necessary to avoid having to modify the existing access logging arrangements which are shared with other PA sub-systems

The Contents of the Microfilm Archives

The microfilm archives are to be converted into digital form, and all of their functions are to be subsumed into the ROP database system. The contents of the archive will continue to be of the nature of a photographic image, and will be human-readable, but the text that the documents contain will not become machine-readable as a result of the conversion.

The more recent and active films would be converted prior to the commencement of the re-issue of cards. The conversion of the complete microfilm archive would require a long period, however, perhaps up to 3 years. A decision will be taken later as to whether, when and how to dispose of the microfilm.

Remaining indexes will mostly be converted from their present card or microfilm form into digital form. A few exceptions will remain in micro-fiche form.

The Functions of the ROP Database

The PA(ROP) sub-system, operational in its present form since 1995, requires enhancement or replacement. The key changes include the following, dependent on technical feasibility, policy decisions and costs[19]:

- replacement registration processes;
- equipment and associated processes for the capture of digital photographs and digital images of the left and right thumbprints;
- equipment and associated processes for the digitisation of application forms and supporting documents, and of notifications of changes of particulars;
- card personalisation, card issue and card management processes;
- enhanced Shroff processes;
- enhanced enquiry and display functions;
- monitoring of enquiry transactions in order to detect anomalous activities, e.g. enquiry by a Registration Officer without an application being processed that day, and amendment of a record in which the Deceased Indicator is set;
- augmentation of the Chinese Commercial Codes (CCC) by 2-byte Unicode (ISO10646) representations of Chinese ideograms. (CCC cannot be simply replaced, because other sub-systems of PA and the TDIS system both use it).

The uses of the digital thumbprint are explicitly to be restricted to one-to-one comparisons for the purpose of authenticating a claim of identity by a person. They are not to be used for any other purpose, and, in particular, are not to be used for one-to-many comparisons in order to identify a person from their thumbprints.

Additional Elements of the Scheme

Additional elements will need to be installed as part of the scheme, including:

- card-personalisation and validation facilities available to ROP registration offices;
- digital photographic facilities at ROP registration offices;
- digital thumbprint capture facilities at ROP registration offices;
- card database management software and a Smart Card Scheme Operator. The FS Report envisages that this function might be performed by a government agency external to ImmD to facilitate the card's use for additional, external purposes;
- digitisation facilities to convert the existing microfilm archive into a form whereby it can be stored on and accessed using ImmD's computer services;

[19] Preliminary specification for the functions are in the Feasibility Study Report, Part I, pp. 29-49, and Part II, pp.35-217

- enhanced display devices, to enable display of photograph and thumbprint images;
- if digital signatures are supported, then:
  - a complete public key infrastructure will have to be available, including certification authorities and registration authorities. At present the only service available is that of the Hong Kong Post Office. It is not envisaged that ImmD would itself perform these roles;
  - all elements of ImmD's communication networks would need to support encryption and decryption.

The Card Issue Processes under the New Identity Card System

The envisaged issue processes for the new card are as follows[20]:

- the applicant makes an appointment in advance - for the replacement exercise, within a period designated for the category of applicants to which the applicant belongs;
- the applicant comes to the ROP Registration Office at that time or for walk-in applicant, come at any time and their application will be handled subject to availability of quota;
- the applicant brings any required documents and the old card (if the applicant has one);
- the applicant queues at the Reception Counter;
- the applicant collects a partly pre-printed and bar-coded form, and completes the form;
- the applicant awaits call by a Registration Officer;
- a Registration Officer:
  - calls the applicant to their desk;
  - conducts initial checking of forms and against the database;
  - captures the person's photograph using digitising equipment;
  - captures the person's left thumbprint using digitising equipment;
  - captures the person's right thumbprint using digitising equipment;
  - digitises the documents that the person presents (i.e. the application form and any supporting documents);
- the applicant awaits call by an Immigration Officer;
- an Immigration Officer:
  - calls the applicant to their desk;
  - checks the person's left thumbprint against the digitised version read a few minutes earlier;

[20] described in the Feasibility Study Report, Part II, pp.79-85.

  - conducts an interview, and checking of forms and against the database, as appropriate to the nature of the application;
  - confirms the residential status and approves the application;
- the computer system prints an Acknowledgement Form;
- the applicant awaits call by a Shroff Officer;
- a Shroff Officer**:**
  - checks the person's appearance against the photo on the relevant ID card;
  - collects any fee required;
  - issues the Acknowledgement Form.
- the applicant leaves the ROP Registration Office**.**

An application verification process is undertaken similar to the current process (primarily to check that the thumbprints on the current and on the most recent application are the same).

The card personalisation process is undertaken (in-house rather than by the Government Printer as at present).

The application and issue process will continue to require two visits - the first visit for registration and the second visit for collection. Although cards could be produced on the spot, they will only be personalised at a central site for improved security control. The target time before collection will be 10 working days after the first visit at the start but will probably shortened after the system is fully operational, compared to 15 days at present.

At pickup time, the person or their proxy queues at the Issuing Office. Checks are performed of the person's thumbprint, the Acknowledgement Form, and (in the case of proxy pickups) other documents provided. The card is issued.

The process for subsequent card application and issuance will be the same as that described above. However, since the digital image of thumbprint is already in place, the verification process will be much simplified.

Infrastructure to support Re-registration and Card-issue

The first bulk re-issue occurred in 1960, with the successive new cards replacement exercise introduced in 1983 and 1987 Both of those HK-wide identity card replacement exercises took 4 years to complete and over 4 million cards were issued during each exercise.

The re-registration and card-issue process will involve the 6 existing ROP Registration Offices and 7 ID Card Collection Offices being supplemented for a period of time by 9 New ID Card Issuing Offices (NICIO). The Feasibility Study Report envisages that the existing offices (around 100 'Registration Desks' and 40 'Assessment Desks' (i.e. Immigration Officers)) would be supplemented by a further

175 Registration Desks and 65 Assessment Desks[21]. A total of 8,325 applications (2,325 for normal ROP applications and 6,000 for replacement applications) per day or 48,740 per week (12,740 for normal ROP applications and 36,000 for replacement applications) will be processed.

It is projected that re-issue would require 4 years, commencing in 2003, and that the NICIOs would operate throughout that time.

A mobile team would perform the functions of an NICIO in remote areas (e.g. outlying islands).

The life of smartcards is likely to be limited, to perhaps 5 years at most[22]. This is because a new form of wear-and-tear arises from contact with card-receivers, and frequent use of card at control points will be particularly hard on cards. Hence re-issue processes may be more frequent than in the past.

The Circumstances of Application for, and Issue of, the Card

It appears that, at least initially, the circumstances under which people will apply for, and will be issued with, the HKSAR card, will differ little from the current scheme. One additional factor will be more frequent application for a replacement card, due to the increased wear-and-tear involved in the new scheme. Each additional visit would appear to be likely to be similar to visits under the present scheme.

If any of the envisaged additional uses of the card were to eventuate, multiple additional circumstances could well arise in which re-issue might be needed and/or the card might need to be presented in order to enable modifications to be made to the data/software specially designated for such use.

Authentication Procedures

It is envisaged that authentication will differ from the current scheme in the following ways:

- the image of the person's photograph that is stored on the card (or possibly that stored in the ROP database) will be able to be displayed on a screen, providing a larger image for comparison against the person's present appearance;
- the person's left thumbprint will be checked against that stored on the card (the template is also stored in the ROP database, but there is currently no intention to use that for comparison purposes). This will be performed under various circumstances, including:
  - by policemen on the beat and immigration investigation officers in field conditions, to authenticate the card holder's identity;
  - possibly by many other agencies, which may well seek authority to perform authentication in the same manner, for a wide variety of purposes;

[21] Part II p.124
[22] See FS Market Research Report 3.1.1.10 at pp.19-21; 5.2.7.3 at p.59; and 5.5.10 at p.165.

- possibly by other organisations, such as employers, which may well seek authority to perform authentication in the same manner, for a wide variety of purposes.

ImmD does not intend to commence authentication of any of the large number of self-reported data-items.

Security Measures

It is envisaged that the security measures in the current scheme will be sustained, and enhanced in the following ways:

- within the card:
  - several items will cease to be displayed in visible form on the card;
  - the data and software stored on the chip are to be subject to hardware, systems software and cryptographic protections;
  - the thumbprints will be stored in the form of a template rather than as a digital image. The conversion will be by means of a one-way hash algorithm. The conversion is irreversible and no thumbprint could be reproduced from the template;
  - if digital signatures are to be supported:
    - key-generation may be performed on-card;
    - key-storage may be certifiably secure;
    - use of the digital-signature private-key may be precluded unless the person is reliably authenticated;
  - if asymmetric encryption is to be supported, the private key may be subject to the protections noted above for digital signatures;
  - if additional applications are to be supported, the segregation of application zones or regions may be protected by hardware and/or systems software or by application features;
- within the card-receiving device:
  - the device architecture may feature security access modules (SAMs);
  - devices that involve capture of a thumbprint may include a secure thumbprint capture-pad;
  - devices that involve capture of a PIN may include a secure PIN-pad;
  - between the card and card-receiving devices:
    - two-way device authentication may be performed;
    - the card may authenticate the device's authorisation to make the particular kind of request.
- within the ROP sub-system:
  - a more intensive record of accesses to records is to be implemented;
  - some limited automated analysis of anomalies is intended to be introduced.

The Circumstances of Use of the Card

ImmD

It is envisaged that the new card will be used more often than the previous card. This is because of its application to such additional purposes as Automated Passenger Clearance and for cardholders to check the contents of their cards and, possibly, to authenticate messages to ImmD (assuming digital certificate capability); to amend the PIN; to update the card software; and for a variety of additional applications that are under consideration.

The new cards will be placed in card-reading devices, for such reasons as:

- to automatically acquire the card number and thereby automate access to the ROP database;
- to ascertain details such as limit and condition of stay which are held on the chip but not displayed on the face of the card; and
- to read the thumbprint template, in order to automatically compare it with a thumbprint taken at the scene.

The cards will therefore be subject to more use than before, and to contact with card-receivers, which creates more wear-and-tear. Moreover, the new cards have additional failure-points, in the form of the chip and the contacts[23]. For these reasons, the new cards will need to be replaced more frequently than the existing cards. Cardholders will therefore be required to present at ImmD Registration Offices more often than with the existing card, and those Offices will need to have the capacity to cope with the increased volume of visits and card-issues.

The Police

The interface between the PA/ROP system and the police ECACCS system is due to be replaced around 2004 by a new command and control system. The nature of the interface between police systems and new ROP System is intended to remain largely unchanged, giving the police access to a search function similar to that currently in use. The main planned difference is that the authorisation of requests for, and the delivery of document images will be automated, replacing the phone/fax method of microfilm record delivery.

The police have also expressed interest in obtaining information about limitation and conditions of stay directly from the cards, although this would require police to be equipped with card-receivers.

If and when they acquire card-reading equipment, the police will be able to access internal data, especially the COS and LOS and authenticate the card holder's identity by thumbprint. ImmD asserts that the authenticating process will be performed only when there are reasonable grounds to suspect the bona-fide of an identity card holder. Otherwise, they would be restricted to visual inspection of the card, with the option of a telephone or electronic request for further particulars, through the appropriate channels.

[23] See FS Market research 5.5.10, p.165.

Other Government Agencies

ImmD believes that other government agencies authorised to inspect the card and other organizations that choose to do so, will probably continue to use the new card in the same way as they do the current card. There is no suggestion that any of these other agencies plan to make a case for the installation of card-receivers.

All government agencies have been invited to submit bids for smart-card applications to the separate ITBB led steering committee. Details of what if any bids may have been made for additional functionality were not available to the consultants of this PIA Report.

Other Organisations

A large number of non-government organisations also use the card, such as all employers and financial services providers. No suggestion has arisen that the circumstances and mode of use by any of these organisations would change.

The Circumstances of Use of the Card-Number

In the context of the proposed new identity card system, no changes are envisaged in the circumstances of collection and use of the card number. If the Code of Practice continues to apply unchanged, the few limits to recording of card numbers and copying of cards as currently exist may be sustained.

The Circumstances of Use of, and Disclosure from, the ROP Database

Because the database will contain the imaged documents previously stored on microfilm, this section needs to compare future uses with the uses of both the microfilm archive and the ROP database under the existing system.

In the context of the proposed new identity card system, the main change will be the ability of ImmD, either for its own purposes or on behalf of the Police and other agencies, to retrieve the images of application forms and associated documents. This will, for instance, allow much quicker and easier access to the addresses and telephone numbers given at the time of application, or notification of changes. Address information will progressively become out of date, unless it is decided to significantly increase enforcement of the notification of changes requirement under the Ordinance (ROP Regulation 18). Telephone numbers, on the other hand, are increasingly stable, as a result of number portability having been implemented for both fixed line and mobile phones.

A further significant difference is the provision to REO of change of address information in digitised form.

The COS and LOS are originated from the P&V sub-system of ImmD. These will be used only for the purposes of downloading to the card when the person presents to the P&V Division. It is proposed that the P&V Division will have card-receiving

devices that are also able to update COS and LOS on the card. Such devices may also be installed at control-points.

The Circumstances of Subject Access to the Card Data and the ROP Database

It is envisaged that the data subject will be permitted access to data stored on the card, by means of kiosk facilities, which will "allow cardholders to view all personal data stored on their cards, free of charge, with access control by means of biometric user authentication" This would presumably be done by testing a newly-measured left thumbprint against the thumbprint on the card and after authenticating the identity, displaying all information stored in the card – the display clearing after the card holder cancels it or removes their card.

Kiosk access would not allow the card-holder to any information in the ROP database that is not held on the Card chip itself. Access to this information by the individual concerned would continue to be only by a formal written application (see section on Subject access in Part V.)

Underlying Infrastructure

It is envisaged that the underlying infrastructure will differ from the current scheme in the following ways:

- card personalisation is likely to be moved back in-house;
- microfilm operations are to be phased out, probably starting from about 2003 when production of microfilm ceases and finishing in 2005 when all microfilm records have been converted;
- the computer-based ROP database and sub-system are to be re-developed. In line with the increasing tendency towards outsourcing, it is envisaged that the development of the replacement system will be outsourced, and managed by ImmD. ITSD is to provide an advisory service to ImmD, and will have close involvement in order to ensure that the interfaces to other systems are sustained;
- computing and networking resources will be substantially enhanced, and the primary responsibility is to be passed from ITSD to ImmD;
- the new system is to involve additional devices, such as digital cameras, digital fingerprint-capture devices, and card-receivers in the hands of police and immigration investigation officers, and kiosks. These would be the responsibility of ImmD, in consultation with ITSD, and with other affected agencies, particularly the Police.

Special Arrangements

It is understood that there are no plans to make any special arrangements for persons-at-risk or otherwise needing additional privacy, beyond those currently applying.

PART IV – CONTEXTUAL ANALYSIS

Legal Analysis

The Immigration Department, like all other HKSAR agencies, is subject to the Personal Data (Privacy) Ordinance (Cap 486). That Ordinance is not intended to, and does not, place major constraints on new government initiatives involving personal information. Like most privacy or data protection laws around the world, it is essentially a 'good housekeeping' regime with an emphasis on openness and transparency. The requirements of the Ordinance 'lock on' to uses and disclosures of personal data that are necessary for the performance of lawful functions. Government agencies do not necessarily need specific statutory authority for their collection, use and disclosure of personal data provided that they are directly related to a function or activity of the agency concerned (Data Protection Principles 1 & 3).

This does not of course mean that properly authorized government initiatives do not raise broader privacy concerns – or even that they do not raise personal data privacy concerns. The initiatives must still comply with the detailed provisions of the Personal Data (Privacy) Ordinance - including not only the Data Protection Principles but also any Codes of Practice, and the Data Matching controls in Part VI. Initiatives may also, as in the case of the HKSAR ID Card, raise concerns which go beyond technical compliance with the Ordinance and which can only be resolved at the policy level through the political process. In recognition of these wider concerns, the Privacy Commissioner for Personal Data is given functions of researching and commenting on any matters which affect 'the privacy of individuals in relation to personal data'[24] as well as supervising compliance with the Principles. It is in pursuance of these functions that the Commissioner and his Standing Committee on Technological Development have already offered comments on the proposed HKSAR ID Card scheme, and will be consulted as the project continues.

The new card scheme must of course also be implemented in accordance with the relevant functional legislation - in this case primarily the Registration of Persons Ordinance and its Regulations and Part IV of the Immigration Ordinance. The Feasibility Study report touches in several places on the possible need for changes to the ROP Ordinance and Regulations to govern the new elements of the proposed system (eg: Part One s.8; Part 2 s.20.3.6). While this PIA must necessarily assess the need for any such changes required to comply with the Personal Data (Privacy) Ordinance (eg: authority for particular uses or disclosures), it is also appropriate to review existing compliance with the Personal Data (Privacy) Ordinance, for those elements of the new Card scheme which will not change. As with most organizations, there are likely to be some respects in which compliance can be improved. In order to assess the privacy impact of the new system, it is necessary to look both at the new elements and at those processes and activities which will remain the same.

[24] Personal Data (Privacy) Ordinance, s.8(1)(d)(f) &(g).

In the Privacy Impact Analysis section of this report, the assessment of compliance with the Personal Data (Privacy) Ordinance is made under the same broad headings as the Data Protection Principles; ie: collection, quality, use, security, transparency and access.

Authority for disclosure of information from the Microfilm records and ROP Database

Under the ROP Ordinance, the authority for disclosures of information provided by applicants (both urgent and non-urgent as described above) is written permission of the Chief Secretary pursuant to ROP Regulation 24. It is understood that such permissions are generally issued by the Secretary for Security, under delegated authority from the Chief Secretary.

A permission to disclose under ROP Regulation 24 is required to allow disclosure even where the agency or organization to which the data is disclosed has a power or authority to request or require it, unless that power is in *primary* legislation (e.g. the Jury Ordinance), in which case it overrides the disclosure prohibition in the ROP Regulation 24, which is only *subordinate* legislation.

A comprehensive list of permissions is not publicly available, but the Department assured the consultants that the conditions under which the information is released and the nature of ROP information to be released are in accordance with the Regulation 24 permissions. A summary provided identifies the following current disclosures:

- in relation to the recovery of government revenue, all agencies, with the request signed by any officer at the level of Assistant Director or above;
- in relation to criminal prosecution of the person concerned, all agencies, signed by any officer at the level of Assistant Director or above.
- in relation to the investigation of crime or complaints. Examples include:
  - the Hong Kong Police Force;
  - the Independent Commission Against Corruption (ICAC);
  - the Securities and Futures Commission (SFC);
- in relation to the execution of official duties, and other purposes. A number of agencies fall under these headings. Examples include the Registration and Electoral Office (REO) and the Social Welfare Department in relation to missing persons.

In addition, ImmD recognises the need for specific permissions under ROP Regulation 24 for disclosures to the successful tenderers and contractors for the new scheme[25]

ROP information governed by Regulation 24 includes the photograph and fingerprint obtained from the applicants and the information provided by them under Regulation 4(1)(b). ImmD considers that it also includes information provided under Regulation 18 by individuals as changes or updates to the information provided under

[25] see Feasibility Study Report, Part 1, 8.2.4

Regulation 4(1)(b). However, it does not apply to information generated by the Immigration Department itself such as the ID Card number itself, various codes and the microfilm reference, although the latter two are intended for internal use only and generally not disclosed to outside bodies; or to information obtained and recorded from other sources.

Although Regulation 24 prohibits unauthorised disclosure, there is no related offence provision.

All Immigration Department officers and staff are subject to the Official Secrets Ordinance (Cap. 521), which makes it an offence to make unauthorised disclosures of certain types of information, e.g. security, intelligence and defence information and information related to international relations and the commission of offences and criminal investigations (sections 14 to 17 refer). The OSO would not generally apply to disclosure of *information* from the ROP system, although it would apply to unauthorised release of actual *documents* (s.6).

Any unauthorised disclosure of personal data from these sources is likely to be contrary to DPP 3 of the Personal Data (Privacy) Ordinance (Cap. 486). However, a breach of DPP 3 is not itself an offence (section 64(10) of the PDPO refers). Breach of a data protection principle is an offence only if a data user commits the breach in non-compliance with an enforcement notice issued by the Privacy Commissioner for Personal Data.

Data Matching

Apart from the exchange of data between ImmD ROP Sub-division and the REO, described above, there appear to be no other matching procedures undertaken, in the sense of a matching procedure as defined under section 2 of the Personal Data (Privacy) Ordinance (Cap. 486). In general terms, such a procedure usually involves the disclosure of bulk quantities of personal data records collected for one purpose for matching by another organisation against their own records collected for another purpose with a view to taking adverse action against individuals as a result of the matching, e.g. withdrawal of social security benefits when the match reveals loss of or no eligibility for the benefits concerned. If any new such procedures were proposed, they would effectively require the consent of the Privacy Commissioner under s.30 of the PDPO.

Stakeholder Analysis

In the proposal for this PIA, and in subsequent discussions, the authors identified several groups of stakeholders; i.e. persons or organizations with an interest in the HKSAR ID Card proposal. These include:

- ImmD itself - various Divisions*
- ITSD (as service providers to ImmD)*

- Other existing major 'partners' or users of the ID Card - specifically the HK Police*, the Registration and Electoral Office (REO)* and the Jury Unit of the High Court.
- Relevant Policy Bureaux*
- Other organizations which use the HK ID Card as a means of identifying individuals (effectively all organizations in both the public and private sectors in Hong Kong, and some foreign authorities)
- The HK public, and various bodies representative of the general public or special interest groups.
- Legislators
- The Privacy Commissioner for Personal Data*

* The authors of this PIA Report met with those stakeholders marked with an asterisk above during a visit to Hong Kong in August. The schedule of meetings is attached at Appendix 4.

While it has not been possible in the timescale allowed to consult with all of the stakeholders, the authors have tried to take into account what is known of their interests. Other processes, such as the LegCo Panel meetings, and public reporting of them, has provided and will continue to provide for wider input.

Public Attitudes Analysis

Ideally, the privacy impact assessment of the HKSAR ID Card proposal would have been able to draw on research in public attitudes in Hong Kong to the specific proposal for a new card. However, no such targeted surveys have been conducted and the timescale of the PIA did not allow for any fresh research.

There is however, clear evidence of the attitudes of the Hong Kong populace to privacy issues in general, and even to a limited extent on the existing use of the ID Card number. The Privacy Commissioner for Personal Data has commissioned survey research by the University of Hong Kong Social Sciences Research Centre since 1997. The latest opinion survey, carried out in March 1999, confirmed generally high, but not rising, levels of concern about privacy of personal data[26]. When asked specifically about the use of the ID Card number, 42% of individuals had become more concerned about its use, although 58% thought that organizations were more careful in handling the numbers than 12 months previously. Supporting this latter finding, the survey also found high and rising levels of trust in most organizations, including government departments, which received a higher 'trust' score than most other organizations.

Survey research into public attitudes to privacy in other jurisdictions[27] generally confirms a consistent pattern in most developed societies. Privacy of personal data is rated highly as a social concern, and is an increasingly important issue in relation

[26] 1999 Opinion Survey: Personal Data (Privacy) Ordinance: Attitudes and Implementation - Key Findings, Office of the Privacy Commissioner for Personal Data.
[27] See http://www.anu.edu.au/people/Roger.Clarke/DV/Surveys.html

to electronic commerce and electronic service delivery. While a majority of the public are relatively trusting - particularly of government but less so of businesses - a significant and active minority are suspicious of the growth of a "surveillance society" in which individuals' activities, transactions and movements are increasingly recorded and available for analysis and profiling. There is strong support even from the 'trusting majority' for safeguards such as those embodied in the Data Protection Principles, but also a growing demand for increases in the level of surveillance to be minimized, and where unavoidable, publicly justified.

It is also clear from experience elsewhere that public opinion on privacy issues is quite volatile - government or private sector initiatives which are seen as privacy invasive and are taken up as such in the media can quickly provoke major public opposition and become 'symbolic' issues about the power of the state (or of big business). This has been particularly true of identification schemes, even though the 'base' level of cultural acceptance of ID systems varies widely (see below for examples from overseas).

International Experience

As noted above, the introduction or enhancement of national identification schemes has been controversial in some countries, although not in others. Many developed countries have population registration and/or ID cards, and there appears to be no particular correlation with the political system; ie: liberal democracies are just as likely to have such schemes as authoritarian regimes, and there has been strong opposition to such schemes in some countries with histories of instability and even military rule.

Brief summaries of the position in a number of jurisdictions have been compiled and are presented in Appendix 5. Each country report follows the same sequence - a description of any existing or proposed population registration and/or ID card scheme; followed by an account of any privacy safeguards, and a history of any public debate about the scheme.

Public opposition to ID card proposals in the UK, Australia and Canada is particularly relevant to Hong Kong because of the strong links between Hong Kong and those countries, but it should be borne in mind that none of them have the tradition of a significant population registration scheme, and that consequently ID card proposals have been seen as a radical innovation.

Perhaps of even more relevance is the experience in:

- France, where, despite the existence of a long established population register and paper ID cards, proposals in the late 1970s for a new machine readable card met with strong opposition and have not yet been fully implemented;
- Korea, where despite an existing ID card, plans for a multi-function smart card replacement in the late 1990s led to strong public opposition, and the withdrawal of the proposals;
- The Philippines, where a proposed National Computerized Identification Reference System was ruled unconstitutional, on privacy grounds, in 1998;

- Taiwan, where a 1997 proposal for a multi-function ID smartcard was withdrawn after protests and hearings on privacy implications.

In contrast to these examples of public controversy, it should be noted that Singapore and Thailand already have machine readable ID cards which appear to be accepted without protest by most citizens, and Brunei and Malaysia have very recently introduced multi-function ID smart cards, again apparently without any significant public opposition. However, in comparison to these countries, Hong Kong people have a relatively high level of awareness of their rights and freedoms and are sensitive to developments that could diminish or otherwise adversely affect the rights and freedoms they currently enjoy.

PART V - PRIVACY IMPACTS ANALYSIS

This part of the report analyses the privacy impacts of the proposed system. Rather than make specific recommendations, the consultants have reached certain conclusions about the level of privacy risk, and indicated ways in which ImmD, or in some cases the government more generally, can address these risks. Some specific suggestions have been made in the form of "... should …" while other possible solutions which have been left as discussion points.

Brief Overview of the Privacy Impacts of the New HKSAR ID Card Scheme

The existing scheme, by its nature, involves very substantial privacy impacts, but these seem to have been generally accepted by the Hong Kong population. The legislature has recognized the privacy implications of the ID scheme both directly, by requiring the Privacy Commissioner to issue a code of practice on the ID Card Number, and indirectly by requiring approval by the Commissioner for any matching procedures that might make use of the Card number (in addition to general compliance with the Data Protection Principles.

The replacement HKSAR ID Card scheme has substantial further impacts on privacy, and it remains to be seen if these arouse any major concerns, or cause people to question aspects of the existing ID Card scheme.

The following broad factors (some of which are shared with the existing scheme) contribute to the significance of the HKSAR Card scheme in terms of the privacy of the Hong Kong population:

- the mandatory nature of the card;
- the extremely wide range of uses of the card and card-number both within government and across the entire private sector;
- the "mystery" inherent in chip-based functionality and data;
- the significant increase in the categories of data that will be held on-line, as either data or images, rather than, as now, on microfilm;
- the increased use of biometrics, especially the storage of uncompressed thumbprints on the ROP database;
- the increased ease with which existing functions will be undertaken;
- the proposed design of the new card to support additional applications, without at this stage any clear decisions about the nature of those applications.

In the consultants' judgement, the greater ease of use of the new system will inevitably lead to greater volumes of usage for existing purposes, and to pressure to allow its uses for additional purposes. Design of the new card to accommodate other applications, whether or not they are specified or unspecified at this time, effectively recognizes that at least some of these will follow.

On the other hand, an upgraded ID card system should bring some privacy advantages in terms of security and protection against ID fraud and against unauthorized access to personal information.

General Privacy Implications

Objectives of the Scheme

The scheme's usage has broadened very substantially since its inception with the primary purpose of combating illegal immigration. The card and card-number are now used by most government agencies. This has reduced the privacy enjoyed by the Hong Kong population, by facilitating linkage and transfer of data between agencies. The extent to which this opportunity has been taken by agencies, and to which data is transferred using the ID Card number as a matching key, lies outside the scope of this report. The population has however generally accepted the justification for current government uses of the ID Card. ImmD asserts that it is widely seen as providing a convenient way of confirming identity.

The card and card-number are also used extensively by non-government organisations. Although not an objective of the scheme, this has become commonplace. This has also reduced the privacy of the Hon Kong population, by providing corporations with enhanced capabilities to assemble profiles on the various kinds of individuals with whom they deal (such as consumers and employees). The limits that the Privacy Commissioner's code of practice place on recording of the HK ID Card number do not prevent profiling. It is the ability of organizations to uniquely identify individuals with whom they deal, by requesting production of their ID Card, that provides that opportunity. It is not clear to what extent that opportunity has been grasped by corporations to date, but without controls, it is likely to become increasingly common. Use by the private sector has been permitted, and appears to have been generally accepted by the populace, although the Privacy Commissioner's surveys shows rising level of concern about card number use (see section in Part IV on Public Attitude Analysis).

The immediate objectives of the new scheme are to replace all existing cards with new ones with enhanced security features, and to replace aging in-house technologies, thereby enhancing the efficiency of ImmD's ROP processes. These features give rise to many additional privacy impacts, both negative and positive. They are analysed in detail in the following sections of this document.

Many possible extensions to the scheme are being considered through a separate inter-departmental process of which the consultants have only limited knowledge. This process is focusing particularly on additional applications for a smart card, some of which may be considered for placement on the new HKSAR ID Card. Some of these applications may be of interest to ImmD, but many are relevant only to agencies other than ImmD. The various initiatives are all highly immature at present. Their privacy impacts are highly likely to be considerable, not least because of their inevitably close association with the comprehensive population registration scheme; but the impacts cannot be fully assessed at this stage.

ImmD is proposing to provide infrastructure to support such additional applications of the card, in particular digital signature facilities and excess capacity on the card. The infrastructure design will substantially determine the extent to which, how, and with what kinds of protections, such additional applications might proceed. It is accordingly essential that the privacy impacts of the infrastructure be considered in the sections that follow, even though the impact of actual applications cannot be.

An individual's registered name is required to be used in all dealings with all government agencies, and the effect of the existing scheme is that that name, which appears on the ID Card, needs to be used with all of the many organisations that demand the card and/or use the card-number. This effectively precludes the use in many economic and social activities of aliases and hence of pseudonymity. ImmD asserts that this is not seen as a negative consequence by the Hong Kong public. Unfortunately there are no research findings to confirm if this is the case or not. No change is envisaged in these aspects of the scheme or legislative framework.

Legislative framework

From a privacy perspective, it is desirable for the objectives of the HKSAR ID Card system to be expressly specified in law. The current situation, where there is a statutory framework for Registration, and for access to registration data; but where the uses of the Card and Card Number are not defined and only loosely controlled, is unsatisfactory. A comprehensive statutory framework for the ID Card system as a whole, including registration and uses of the card and card number, would provide important privacy protection, and give re-assurance to the HK population in the face of concerns about 'function creep' and increased surveillance. It would also clarify and remove any uncertainty over the authority for specific uses and disclosures.

Ideally, the statutory framework for the ROP/ID Card system should be reviewed to ensure that it provides a comprehensive basis for the HKSAR ID Card system as a whole, including both registration and card and card number use.

Population Registration

The current HK ID Card scheme does not involve a constantly updated population register with current details of addresses, employment, marital status etc. There is only a limited need for such a register for ImmD purposes. This is a very privacy-positive feature of the existing scheme, and expressly confirming it for the new scheme would dispel many privacy concerns. However, the requirement to notify changes of registered particulars (ROP Regulation 18), while it is not generally enforced, suggests that the policy objective of the ID Card scheme is not just to issue individuals with proof of identity but to also to maintain a population register with, if resources allowed, up-to-date contact and location details.

Privacy concerns need to be seen not just in light of the current state of ROP Information, but also in light of the prospect of an much enhanced population register, which would become a much more attractive resource for other uses. If ImmD would like to move towards a more regularly updated population register, this is likely to be seen as a development providing more for the needs of other agencies,

which would be a clear example of ‘function creep’. Such a development would also be likely to increase concerns about the potential use of registration information for population monitoring and surveillance.

Multiple applications

It is self-evident that the further along the path from a single-purpose, non-smart ID card towards a multi-function, contactless smart card the HKSAR moves, the greater will be the privacy concerns. The best way of satisfying those concerns is to strictly limit, both by law and by technical specifications, the distance along that path that the HKSAR moves. Hong Kong has already moved away from the single-purpose for the card, and it is understood that a decision has already been taken to have a smart card. At the same time, a contactless card has been ruled out, which indirectly provides one important privacy safeguard.

There remains the crucial decision as to whether the new HKSAR ID Card should be designed to accommodate multiple, and as yet unspecified, functions. Simply declaring that decisions about other functions will be taken elsewhere, and subject to legislative approval, does not avoid this being a fundamental privacy issue for the new ImmD scheme. If a decision is made to provide infrastructure on the card for other applications, not required for the purposes authorized under the Immigration and Registration of Person's Ordinances, then ImmD will unavoidably be drawn into debate about the nature and privacy implications of other possible functions. This has already been demonstrated in the comments of LegCo members at the briefings given to the Security Panel on the new card.

If the government was prepared to expressly rule out certain capabilities and uses, attitudes to ImmD's immediate proposal would be far less influenced by debate on other applications. If nothing is ruled out, then public debate on the new card will inevitably encompass all possibilities, and their implications, both positive and negative.

If any additional applications or uses are considered for the HKSAR ID Card, they should ideally be voluntary, ie: entirely at the discretion of the card holder, and not implemented in such as way as to make the choice of the application a practical necessity. It may be that some other government applications (such as the use of the Card as a replacement driver’s licence) may need to be made mandatory, but it should be recognized that it is this prospect which lies at the heart of privacy concerns about ID card systems.

Card management

Any decision to allow card-issue and management to be undertaken by another government agency, or by a commercial operator, would result in a whole host of additional privacy issues arising, particularly in relation to access control, security and authorization of further uses or applications. If the management of the card scheme were to be performed by any organisation other than ImmD, it may give the appearance of a *de facto* decision to extend the scheme’s purposes beyond the

Immigration/ROP functions. Even outsourcing of card issue and management, under strict contractual controls, raises additional issues.

Privacy concerns would be lessened if ImmD retained in-house all aspects of the card scheme management, not only initially but also for the duration of the life of this and successor schemes, and if the possibility of the function being performed by any other government agency, or being outsourced, was expressly ruled out.

Balancing privacy and other objectives

Clearly, privacy considerations cannot be the only, or even the most important, factor to be taken into account in decisions about the new HKSAR ID Card. The purpose of a Privacy Impact Assessment such as this is however to ensure that all of the privacy implications are 'on the table' to be taken into account in the inevitable balancing of public and private interests.

Revision of the cost-benefit analysis already undertaken to take account of non-quantifiable, qualitative or intangible benefits and costs, including privacy, would assist an informed and balanced decision about various scheme features and parameters. Methodologies for dealing with non-quantifiable factors in a cost-benefit framework are available.

Specific privacy implications

The Contents of the Card

There is a significant amount of personal data contained on the face of the card. This is disclosed to many people in many agencies and non-government organisations on each of the many occasions on which it is presented to them. Several of the symbols that appear on the existing HK ID Card will not appear on the face of the new card, and the information they convey will not be held in the chip, which is a privacy-positive aspect of the new scheme.

The indicator that one or more cards have been previously lost appears to provide a basis for generating suspicion on the part of the person handling the card that the cardholder may be involved in illegal activity, even though this is clearly unjustified in the case of individuals who simply lose their card, or have them stolen. This indicator is to be removed from the face of the card and will not be included in the data held on the chip, which is superficially a privacy-positive aspect of the new scheme.

There may however be a significant privacy-negative second order effect. If the Police previously used the 'lost' indicator to compare with information given to them from the ROP database, then its removal might lead them to seek alternative means of checking for irregularities, such as the ability to scan a thumb and compare it with the thumbprint on the card. This would be a very significant adverse privacy impact.

It is envisaged that the new card will contain several additional data-items in the chip, in particular the digital photograph, digital templates of the thumbprints, and the Limit

and Conditions of Stay (LOS and COS). These will be newly available, but only to those persons and organisations that have access to an appropriate card-reading device.

The fact that the new card is proposed to be a smartcard creates additional privacy concerns. The following factors need to be considered:

- the ability of the card to store data that is unknown to the person, may be against the person's wishes, and/or may be harmful to the person's interests;
- the ability of the card to disclose data in a manner that is unknown to the person, may be against the person's wishes, and/or may be harmful to the person's interests;
- the ability of the card to perform functions, and/or to participate in the performance of functions that are unknown to the person, may be against the person's wishes, and/or may be harmful to the person's interests.

The fact that the card is a smartcard would also provide the possibility of some advantages for privacy. The following factors need to be considered:

- to the extent that the card performs challenge to and authentication of devices and processes with which it interacts, the card can provide protection of the data against disclosure to, and of processes from performance by, unauthorised parties;
- to the extent that the card participates effectively in the authentication of the person presenting it, the card can prevent the exercising of the cardholder's prerogatives by an imposter, hence providing some degree of protection against identity fraud. This depends on the authentication mechanism being available to the organisation using the card. If this protection is only based on a PIN, it would not represent a particularly strong form of protection. Protection involving the biometric (thumbprint) would be a considerable improvement, but would involve additional 'intrusion' that may not be acceptable to cardholders;
- to the extent that:
  - the card supports secure key-generation, secure key-storage, and secure key usage; and
  - cardholder choice exists concerning how many key-pairs, and how many certificates are acquired, and which are used under which circumstances;

  the card can contribute to the security of message transmission, and the authentication of messages and hence the prevention of messages from other persons that masquerade as being from the cardholder, again providing some degree of protection against identity fraud. However, since this is likely to depend only on a PIN, it may only be a weak form of protection.

The fact that the smartcard is proposed to be a contact-based rather than a contactless or hybrid card avoids a further privacy concern. To release data, or be involved in the performance of any function, a contact-based card requires the individual to either place the card in a card-reading device, or yield the card to another person. Hence occasions on which privacy intrusion might arise are at least generally apparent to the cardholder. With contactless cards, on the other hand, the perception, and to some degree the reality, exists, that processes may take place entirely without the knowledge of the cardholder.

The Functions of the Card

The smartcard-based approach proposed for the new scheme would provide the card with the capability to perform functions that the existing card could not do. Many aspects of the card's potential functionality raise privacy concerns.

One critical privacy protection is the nature and degree of segregation between and independence of the functions that the card performs. The effectiveness and credibility of that independence is to a large extent determined by whether it is implemented by means of:

- hardware features;
- systems software features; and/or
- application-level features.

The standard that needs to be applied is that no application can be able to compromise any other applications or their associated data; ie: unable to either access data or functions, or use them in any way, without appropriate authority.

It is also very important that the card undertake authentication of card-reading devices, and of processes that request the disclosure or change of data. Only in this way can it be ensured that interactions take place only with the intended devices, and only in the intended circumstances, and only for the intended purposes.

Implications of cryptographic functions

If the cards are to be capable of supporting cryptographic functions, these functions will embody both privacy-protective and privacy-invasive aspects. For maximum privacy protection, private keys, for both digital signature and message-encryption purposes, should be generated on the chip, never leave the chip, and certifiably can never leave the chip.

If, on the other hand, there was a requirement in relation to backup of private keys (for the purpose of their recovery by the cardholder), or escrow of private keys (for the purpose of recovery by some other organisation), this would raise significant privacy concerns.

It would also be crucial that the use of the private keys, both to digitally sign outgoing messages, and to decrypt incoming messages, be precluded unless the person using the card has been authenticated. PINs are a very weak form of protection. Comparison between a measured biometric (such as the thumbprint) and the corresponding chip-stored biometric is a much higher-strength protection.

Two further concerns are that limitations might be imposed:

- on the number of key-pairs, perhaps even to require that the person use the same private (digital signature) key to sign all outgoing messages, no matter who they are to, and to request all correspondents to use the same public (encryption) key to encrypt all incoming messages; and

- on the number of digital certificates held by an individual, perhaps even to require that the person use the same certificate for all purposes.

Any such limitations would negate the potential of public key infrastructure to provide privacy-protection, because they would represent further unique identifiers that could be used to trace a person's activities and consolidate their data trails. It would therefore represent a yet further privacy-invasive aspect of the scheme.

The Functions of Card-Receiving Devices

The introduction into the scheme of card-receiving devices give rise to privacy concerns. These include the following:

- there is a risk of interception of traffic, and hence access to personal data or access to a stream of data that can be replayed later as a means of achieving masquerade. This risk occurs:
  - within the device;
  - between the device and the card; and
  - between the device and any other device with which it communicates, such as a local server, or a remote server by means of a communications router;
- there is a risk of the recorded biometric becoming capturable by other agencies, organisations or individuals. This can arise if the biometric is not adequately protected, e.g. because it is not encrypted, or the hashing algorithm is not one-way, or the compression is insufficiently 'lossy' and hence the compressed form can be used to generate an adequate masquerade;
- there is an increased risk of other organisations seeking to capture the biometric themselves, eg businesses seeking to use the card as an access control device;
- there is a risk of the PIN or PINs being captured;
- in the case of unsupervised devices (such as self-service kiosks), there is a risk of masquerade by imposters who acquire the card and any necessary knowledge such as a PIN, and/or are able to simulate the biometric;
- there is a risk of card-data being amended by unauthorised devices;

It is accepted that some of these risks would only arise if policy decisions were made that are not currently intended e.g. more widespread installation of terminals which could both read and update card data, or on-line links between card receivers and databases. All of the risks can be addressed by the various security measures discussed elsewhere in this report, but most cannot be eliminated entirely.

The Contents of the ROP Database and Microfilm Archives

Currently, the ROP database contains only a sub-set of the personal data gathered from, and generated about, each person. A significant amount of additional data is stored only in microfilm form. This is a very significant privacy-positive feature. The reason is that it represents a form of 'constructive inefficiency', making it labour-intensive, slow and expensive to access the data, and hence reducing the volume of requests and the incentive for other agencies and organisations to seek access to it.

While it is difficult to argue for inefficiency as a policy objective, it needs to be recognized that removing increased efficiency can have incidental consequences.

As a result of the changes being proposed for the new scheme, several items of the enhanced ROP Database represent significant privacy concerns. These include:

- all data provided by, and generated about, persons would now be converted into at least potentially machine-readable form. It is currently envisaged that a great deal of this data, on application forms, supporting documentation, and notifications of change of particulars, would be in image only, and not converted to text. Nonetheless, this measure removes a significant part of the 'constructive inefficiency' inherent in the existing scheme, and thereby increases the risks of increased volumes of requests for access and of function creep;
- the storage of biometrics in the ROP database, access to them, and consequential storage in multiple levels of server and temporary server cache are a serious concern. This is because storage of a biometric anywhere creates the risk of escape to other organisations and individuals, and hence of masquerade. A biometric is analogous to a PIN that can never be changed, and is therefore very sensitive indeed, because at least potentially, and probably already in practice, a convincing copy can be synthesised from such a print. There is rapidly increasing awareness of this risk, and in some cases action to reduce it. The project to replace the social security card in Spain for example, involves storage of a biometric on the card, and only on the card. The proposed encryption and access controls only partially address these concerns;
- it is understood that it is not proposed to convert addresses or telephone numbers into machine readable form – they would be held only in the digitized image of the application form. This will have the privacy positive consequence that the change of residential address data currently keyed for transfer to the REO (where the individual has requested this) will no longer be needed – the relevant digitized images will be transferred to the REO which will do its own conversion. It would however be a very significant development if details such as address and telephone numbers (both residential and college/office) were not merely digitised and hence stored as an image, but also converted into machine-readable (e.g. ASCII) text and stored, becoming available for automated search, access and disclosure in that form as well. The reason is that this would greatly increase the attractiveness of access to the ROP database to other agencies, and to other organizations. ImmD has in the past resisted pressure to make addresses more readily available to other agencies;
- other data-items provided by the individual are also at risk, particularly marital status, spouse's name and card-number, and profession/occupation;
- other database items are also of potential concern, in particular, the Non-Routine Indicator. This is turned on during the application process to signify special cases such as residential status to be established, need to retake thumbprint or need to retake photo etc. After the follow up of the irregularities, the supervisor will turn off the indicator. The indicator is only "Y" or " " and carries no specific meaning. Supervisors will have to refer to the case file/application form for the details. However, while this indicator is set it represents an additional item of data which needs to be protected.

- person-to-person linkage is a very privacy-invasive aspect of the scheme. At present, within the ROP database, actual linkage only exists in relation to the parent/guardian of every minor, and a potential linkage exists in relation to the spouse of every cardholder. ImmD already makes good use of these linkages, for instance to contact a family member in the event of difficulties when an individual is travelling overseas. Some outside agencies also take advantage of these linkages through requests for microfilm records. There is an increasing volume of requests for associated person or 'family tree' information, especially from the police. Once these records are digitised, the improved response times may lead to a substantial increase in associated persons searches and retrievals;
- the proposed enhancements to the log of enquiries made into each person's data is a privacy-positive feature, but it needs to contain sufficient detail such that anomalies could be detected, investigations undertaken, miscreants identified and actions taken against miscreants. Moreover, it needs to be complemented by actual software processes, manual procedures, powers to discipline miscreants, application of the processes and procedures, and actual disciplinary action.

The Functions of the ROP Sub-System and Manual Procedures

The ROP Offices perform a wide range of functions by means of a mix of computer-supported and manual activities. It is acknowledged that many of these functions support services needed and valued by the public such as the issue of travel documents, while other 'control' functions are accepted as desirable in the public interest

In general, it is envisaged that the new scheme will enable the performance of much the same functions, using modern information technologies in order to achieve resource efficiencies within ROP Offices.

Functions of the ROP sub-system that embody particular privacy concerns include the following:

- for the first time, the ROP sub-system is to include the capability to store and display representations of individuals' appearance (photo) and thumbprints, as well as automated thumbprint matching. Many people may see no significant differences between digital photography and fingerprinting, and the more traditional forms (film, and paper & ink). Others see significant differences, both philosophically and practically (e.g. in the ability to manipulate the images); and
- for the first time, the ROP database is to contain computerised digital images of documents. In the consultant's judgement, this makes the database a more attractive and valuable resource, and increases the likelihood that other agencies and organizations will seek access to the imaged information either directly or through conversion into machine-readable form.

The storage of an uncompressed digital thumbprint in the ROP database gives rise to substantial privacy-intrusiveness and risk.

There appears to be only one usage of the thumbprint in the ROP database. For each application other than the initial one, the new thumbprint is checked against the

one supplied by the person on the most recent occasion that they had a card issued or re-issued. This is currently performed by suitably trained Verification Officers, by comparing the newly-taken ink-on-paper print. In the new scheme, it would be performed initially by auto-comparison between the new and old digital images. At least those comparisons that result in no or relatively low matches will be then checked visually on a display-screen.

Based on figures for 1999-2000, this occurs in about 365,000 cases p.a., i.e for all applications where the person is in transition from one kind of card to another, or needs a replacement card.

In most of these cases, the test could be performed differently: the template of the new print could be tested against that on the card. This would have applied to about 230,000 of the cases in 1999-2000.

The exceptions are those where the card is not available. Again using 1999-2000 figures, this would comprise 130,000 lost cards p.a., and some of the 22,000 p.a. where the card has been damaged or defaced. So there would be perhaps 135,000 cases each year (although this would rise if card reliability and durability proved to be less than is currently anticipated). It is only for these cases that any potential justification appears to exist for storing the thumbprint on the ROP database.

If the thumbprint is not held, the following implications arise:

- each applicant who cannot produce a card that can process the card-stored thumbprint template would have to undergo the full process of establishing their credentials with the ROP Registration Office. This would require some additional documents, and might involve a somewhat longer interview;
- there could be an increase in the risk of fraudulent applications resulting in a card being issued to the wrong person, and bearing that person's thumbprint and photograph. There are considerable controls available to prevent that, however. They include:
  - the fact that the previous card was lost or damaged is known to the officer processing the application;
  - the ROP database contains the real person's photograph, enabling a test of whether the person presenting resembles that image;
  - the ROP database contains the signature provided on the previous occasion(s), enabling a visual (or even machine-assisted) comparison with the signature on the new application;
  - the ROP database contains a significant amount of personal data that can be compared with that on the new application, and which can be used as the basis for questions that the applicant should be able to answer without difficulty;
- the anti-corruption measure of having verification by an officer other than the one that undertakes the interview would be negatively affected. That process could, however, repeat the process already undertaken at the front desk, with the exception of the ability to ask additional questions of the applicant;
- a small amount of additional effort and time would be required of the ROP Registration Officer.

It appears that the omission of the thumbprint from the ROP database would have a limited negative impact (some relatively minor inconvenience for those who have lost

or damaged cards), in return for a very considerable reduction in the system's privacy-invasiveness.

An alternative approach would be for the ROP database to carry only the thumbprint template (which should be based on a proven and published algorithm to ensure independence from particular vendors). The software available to Verification Officers could then perform a comparison of the template of the newly provided thumbprint against that or those already stored.

If the thumbprints are to be stored on the ROP database, despite the privacy risks that entails, then the encryption and access controls will be crucial.

The Circumstances of Application for, and Issue of, the Card

The circumstances in which application will be necessary change a little under the new scheme, and these aspects generate some privacy concerns, as follows:

- the frequency with which people will have to visit ROP Registration Offices will almost certainly increase. This is because:
  - card failure will occur much more often than before (estimates of the failure rate in the Market Research Report[28] relate only to selected factors, and do not include, for instance, damage to chip and contacts);
  - the life of cards generally will be less, necessitating much shorter cycles for re-issue of cards to the whole population;
  - if there were any change to the age(s) at which young people are required to be thumbprinted, in response to concerns about fingerprint instability[29], children (and hence the parent or guardian) may be required to attend an ROP Registration Office more often than before, increasing both the inconvenience to the populace and the volume of transactions needing to be processed by ImmD;
- additional factors could result in even faster increases in the frequency with which people will have to visit ROP Registration Offices. For example, the possibility exists that the requirement for changes in registered particulars, which hitherto has not been enforced, will be, because of the attractiveness to ImmD and other agencies of accurate, up-to-date databases, and of cross-notification. It is mainly resource constraints that have prevented ImmD from pursuing notification of changes – it remains a policy objective.

Although not directly a *data*-privacy issue, increased frequency of visits to registration offices, with the questioning and other data capture involved, will undoubtedly be seen as an adverse privacy consequence of the new system.

Re-registration for the HKSAR ID Card

The scheme will involve mandatory visits by every person who holds a card, rather than progressive replacement of each card only when the need arises (i.e. issue of a

[28] Feasibility Study Market Research Report, pp 19-21, 156-157 and 165.
[29] Feasibility Study Market Research Report, p 163

first card, change of card-type, change of card-details, loss or damage). Given that some card-holders present more than once in any given year, currently less than 7% of the card-holder population presents themselves at ROP Offices each year. The traffic in all ROP /new ID card issuing offices will therefore increase dramatically during the changeover period.

For the first time, the new scheme will include the requirement to submit to machine-reading of, and processing of a representation of, thumbprints and photograph. Within ROP Registration Offices alone, this will arise:

- on original registration; and
- on each occasion that a card needs to be re-issued.

This will be seen by some as an unwelcome and privacy intrusive change, while others will regard it as no different from the existing non-digital photograph and manual/paper thumbprint.

While some of the aged, blind and infirm will continue to be exempted from the need to hold an ID Card, no conscientious objection or other exceptions are allowed amongst those who must hold a card. This means no exceptions in relation to the personal data, the full-face photograph, or the thumbprint, either in the existing or new systems, although some individuals are allowed to wear head coverings due to religious reasons provided they do not obscure the face. The absence of any further exceptions may be seen as insensitive to the needs of those who, for religious or other conscientious reasons, or because of disfigurement, may object, in particular to the taking of a full face photograph in a public arena, or at all.

Capture of the thumbprint currently involves an ROP officer holding the person's forearm, and rolling it, in order to achieve a print of sufficient quality. This is invasive of the privacy of the person. It is understood that the new scheme will require a similar action involving an officer holding the person's arm. ImmD asserts that the assistance is mainly to save individuals the inconvenience, (and additional intrusion) of having to repeat the process if a good print is not obtained. ImmD suggests that the holding of the person's arm is not generally perceived negatively, and asserts that if an individual insists on providing a print unaided they are allowed to do so - although it may take several attempts.

The exemptions from the requirement to have an ID Card for some of the aged, blind or infirm are expected to continue. There will, as now, be almost no other special arrangements to allow for exceptional circumstances. For example, there is no provision for registration without attending one of the fixed Registration Offices, except during the re-issue period when a mobile service will be provided to remote areas and outlying islands. The only special arrangements in relation to the processing of applications and the issue of cards are the ability to apply for an appointment (which merely assures entry and avoids the first queue), and the ability to have a proxy fetch the card when it is ready. This has negative privacy implications for people at risk, or who would otherwise prefer not to be seen in public places.

Notification of Changes of Personal Particulars

It is a requirement in law to notify changes of particulars, and significant penalties are prescribed for breaches of that law. In practice, mainly for resource reasons, the law is not enforced. The fact that it is not enforced is a privacy-positive feature of the existing scheme. On the other hand, the fact that such a law exists is a privacy-negative aspect. It suggests that the policy objective of the ID Card scheme is not just to issue individuals with proof of identity but to maintain a population register with, if resources allowed, up-to-date contact and location details. ImmD asserts that keeping such details up-to-date is, or would be, helpful to most individuals in that it would reduce the frequency of challenges on the basis that registered details no longer corresponded to current circumstances.

The new scheme, by making a great deal of personal data potentially machine-readable for the first time, creates momentum towards greater emphasis being placed on the accuracy and up-to-dateness of that data, and hence towards enforcement of the requirement to notify changes. That would represent a significant increase in the privacy-invasiveness of the scheme, and would lay the foundation for yet more privacy-invasiveness in the form of further access by other agencies and even by other non-government organizations. While such access would need to be authorised by law, the opportunity created by machine readability is likely to lead to pressure for privacy-negative changes.

Security Features

Any ID card scheme will inevitably be subject to some deficiencies in relation to such matters as identity error; identity impersonation, fraud and theft; card issue to the wrong person; and duplication and forgery. Even though the new systems will be expressly designed to reduce error and fraud, it would be unrealistic to expect it to be entirely eliminated. Some limited statistics are available about the existing scheme - ImmD processed between approximately 700 and 2000 cases of abuse a year during the 1990s (this excludes cases handled by the HK Police). There is insufficient information, however, to enable evaluation of the benefits of particular features of the new scheme and their comparison against disbenefits including privacy intrusion.

The existing ROP system embodies a wide range of appropriate access control measures, which (in addition to their primary purposes) represent privacy-positive features.

The interface with the police ECACCS system in particular, is subject to considerable security precautions. These are vital means for achieving some limitations on the degree of privacy-invasiveness of the scheme.

The system lacks any ability to preclude access to the records of particular individuals without special authority. This is a desirable feature in respect of persons-at-risk, but also VIPs and celebrities, whose data is currently accessible by anyone who has access to the database as a whole. Many other jurisdictions offer special protection to government held information about public figures. There appears to be no intention to address this issue in Hong Kong. ImmD asserts that

the strength of the audit trails and general culture of confidentiality mean that there is no need for special treatment, which would in any case be contrary to strongly held views about equity.

An outline audit trail is maintained, and policy requires that it be analysed manually; but no automated analyses are undertaken. The new scheme is to feature enhanced audit trails, at least of the imaged paper records (these trails should be designed to contain all of the data needed to ensure effectiveness of the controls), sustained manual analysis procedures, and additional automated analysis. If implemented and operated on an ongoing basis, these would represent privacy-positive features.

The Circumstances of Use of the Card

Citizens and long-term residents are either required to, or have become accustomed to, produce the HK ID card when dealing with:

- ImmD, variously at ROP Registration Offices and border-points (which is either legally required or may facilitate the provision of services);
- the police, at any time, at any place, without any reason needing to be given (although it must be legally authorized. Police Internal Orders require a reasonable suspicion for checking of idenitity cards);
- all other government agencies (provision of some form of evidence of identity is legally authorised, and request for the card is legally sanctioned);
- all employers (which is legally sanctioned); and
- many corporations, in circumstances other than employment.

There is no current intention to change these circumstances. But for the first time, the new scheme will include the requirement to submit to machine-reading and processing of a thumbprint, by at least some of the users (others will presumably continue to rely on visual inspection of the new card). Beyond ROP Registration Offices alone, this will arise, subject to the enactment of the necessary statutory authority:

- on each occasion a policeman requests it (once they have card receivers);
- each time the card is presented at a location fitted with card-reading devices, (increasingly at control-points);

Additional requirements to submit to machine-reading of thumbprints could potentially arise, as other government agencies, and other organisations, mount cases for access to this aspect of the scheme for more efficient authentication.

Even without any additional applications on the card, the risk exists that a great deal more function creep will occur, variously in regard to:

- the organisations that request the card;
- the circumstances in which the request is made;

- the data that is accumulated in association with the card-number and/or official name;
- the gathering of a measure of the thumbprint; and
- pressure to make the thumbprint-image on the card and/or in the ROP database available to support third-party authentication processes.

While none of this could occur without express legal authority, there can be no guarantee that amendments to the relevant Ordinances will not be made in future.

Any additional applications and functions for the card, completely separate from the ROP & Immigration control context, would of course also increase the overall usage of the HKSAR ID card.

The Circumstances of Use of the Card-Number

The card-number alone conveys almost no meaningful information, which is a privacy-positive feature. The prefix does identify 'imported workers' and 'foreign domestic helpers'.

In addition to the use of the card itself, the card-number is also very widely used. These uses are expressly authorised by law, in the case of all government agencies, and employers, to establish identity, and not prohibited in most other circumstances. This breadth of use represents a major intrusion into individuals' privacy, but one which has become generally accepted by the Hong Kong populace, presumably with varying degrees of comfort (see Public Attitudes Analysis in Part IV).

As noted above, the ability to request a government certified unique identifier, even though recording of the number is subject to some restrictions, facilitates the creation and maintenance of profiles and dossiers, and the consolidation of multiple data trails.

The new scheme could exacerbate this situation in a number of ways, e.g:

- by the existence of biometric images and biometric image templates, which may appear in some transaction records as the sole identifier, but which can be being correlated with the ID card-number; and
- If the card was to incorporate digital signatures;
  - if the cardholder were to be restricted to a single digital-signature key-pair. This would be privacy-negative because it would be straightforward for any party to associate the public key with an ID card-number, and hence every message that a person ever signed could be easily associated with every other item of personal data available to the party;
  - if the cardholder were to be restricted to a single digital certificate. As with a single key-pair, it would be straightforward for any party to associate the certificate-ID with an ID card-number, and hence every message that a person ever signed could be easily associated with every other item of personal data available to the party.

(These negative consequences of key pair/certificate restrictions apply to any device carrying a digital signature, so this is a privacy negative feature that the HKSAR ID Card would share with any other cards carrying digital signatures.)

Scheme Reliability

The present scheme is dependent to only a very limited extent on technology, and most functions can be performed whether or not the electricity supply, networks and computers are operational.

That changes a great deal under the new scheme, because of the extent to which particular functions will be dependent on various technologies. The following factors need to be considered:

- large-scale smartcard schemes to date have been primarily focussed on payment and ticketing, and have seldom addressed ID, especially across the population of a region like Hong Kong;
- smartcard schemes to date have seldom involved multiple applications, particularly large-scale smartcard schemes;
- smartcard schemes to date have seldom implemented biometrics;
- biometrics formats, processing and interfacing are currently proprietary, and standards are only now beginning to emerge;
- smartcard schemes to date have seldom implemented digital signature production, affixing and despatch;
- smartcard schemes to date have seldom implemented on-card key-generation;
- smartcard schemes to date have seldom involved multiple chipcard providers, or multiple card-reading providers;
- interoperability standards are in their infancy;
- failures occur in cards, and in card-receiving devices, including SAMs.

The new scheme therefore has more service reliability risk factors than the existing scheme. Scheme reliability is an issue, not only in terms of service-levels, but also of privacy. In the absence of effective fallback procedures, cardholders will be at least inconvenienced and might also be at risk of additional privacy invasions such as arrest on suspicion, in the event of technology failures. Manual fallback procedures may alleviate this risk but are unlikely to eliminate it entirely.

The standards suggested for availability and resilience are only “at least that of the current system”[30]. ‘Minimalism’ is stated to be the keyword for disaster recovery planning, implying ‘basic survival’ mode[31]. Resilience levels are to be determined later, on the basis of service levels required.

[30] See FS Report Part II, p.39
[31] See FS Report Part II pp.197-206

The scale of privacy intrusion inherent in the registration aspects of the new scheme will depend critically on the durability and life of the cards, and on the reliability of the systems**.** These factors will also have a major impact on the costs of the scheme, against which the privacy implications should be balanced. Unavoidable uncertainty about the life-expectancy and failure rate of smart cards in the HKSAR ID Card application, and about availability and resilience, translates into a privacy risk. If the life of the cards is significantly shorter than expected, or their failure/error rate higher than expected, or the system is unavailable more often, then the privacy intrusiveness of the scheme will increase.

Management & Operation of the Card Scheme

The possibility has been raised, if the card is to hold other applications, of the smart card scheme operator being a separate government agency. ImmD assert that the only proposal under serious consideration is for a very limited range of administrative aspects being handled by another agency, and that ImmD would keep control over all aspects of registration and card-issue.

However, 'outsourcing' of care management implies that a *de facto* decision has already been taken to extend the scheme's purposes beyond ImmD and the control of illegal immigration. It would tend to facilitate further function creep, and further sharing of personal data.

If the smart card scheme operator was a commercial operator, either through 'outsourcing' or as a joint venture, this would raise additional privacy concerns about even more widespread function creep and sharing of personal data, and of potential private sector profiling of individuals.

Circumstances of Use of / Disclosure from the Microfilm Archive / ROP Database

One important change that is envisaged under the new scheme is that access by police would be increasingly automated and efficient. It will therefore become more attractive and the volume of access is likely to rise.

Large numbers of requests made by government agencies are serviced variously through the ITEU, the Confidential Registry, and the Certificates Office. A statistical breakdown of these disclosures is not publicly available; and while steps are taken to ensure that all requests acceded to have been properly authorised, there is no publicly reported auditing as an accountability measure. Under the proposed new scheme:

- as the efficiency of data transfers increases, the extent to which the facilities are used may also tend to increase;
- it may be increasingly difficult to sustain the current restrictions to a relatively small number of officers in each agency; and
- more requests may be made for information about 'associated persons'.

The existing disclosures also encompass, at least in the case of the Confidential Registry, other non-government organisations - the example given being the railway companies in connection with breaches of by-laws. Although these requests are approved on a case by case basis, the new scheme would also enhance the ease and speed of access. The frequency of requests may consequently increase.

A further category of disclosure is the hotline for employers. This also represents an area of risk in relation to function creep – employers could well make a case for access to registration data, particularly if it becomes more up-to-date.

In all of these many instances of disclosure from the enhanced ROP database, the prospect looms of rapid and efficient access to digitised data arising from application forms, supplementary forms and notifications of changes of particulars. This is very likely to lead to more requests for access to more data, more often.

The Feasibility Study Report mentioned a possibility of monitoring of cardholders who frequently cross the border, to determine in advance which cards were most likely to fail as a result of high usage, and call those cardholders in for card replacement on a more frequent basis[32]. ImmD state that they have no intention of doing this – they could already monitor frequency of border crossing through their other systems but do not do so – a privacy positive feature. It would be re-assuring to clearly state publicly that this is not intended as a by-product of the new system.

Special Arrangements

It appears that there will be no provision in the new scheme for most categories of persons-at-risk to receive any special protection in the form of special arrangements whereby they can assume replacement or alternative identities, or suppress or obscure their contact details.

ImmD may wish to consider whether there is a need for special arrangements for persons-at-risk other than protected witnesses. If there is, then changes might be needed to the Ordinance or Regulations to allow for collection of fewer details, suppression of data from normal systems, and/or registration of 'alternative' identities.

The Scope for the Use of Privacy Enhancing Technologies (PETs)

Privacy-enhancing technologies (PETs) are tools designed to counter the impacts of privacy-invading technologies (the PITs). PETs include:

- cookie-management tools;
- anonymity tools; and
- pseudonymity tools.

[32] See FS Market Research Report at 3.1.1.10, p.21 3rd para

The term was invented only in 1995, and is not generally used to encompass basic security features like data and message encryption, although these do of course make contributions to privacy protection.

In principle, PETs could be used in electronic service delivery, for example, verifying eligibility for a social security benefit without identification being required.

In practice, with currently available technology, this is not viable.

Digital signature certification mechanisms are currently based on the CCITT standard X509.v3. This standard requires a 'distinguished name', which is commonly assumed by the designers and users of digital signature schemes to mean 'a person's true name' (whatever that is - in the HK context presumably their registered name).

The X509.v3 standard also introduced an ability to have attribute certificates separately from the underlying 'identity' certificate.

This is an improvement from a privacy perspective, in the sense that a person can present electronic evidence that they are, for example, a qualified medical practitioner, without at the same time unnecessarily disclosing that they are a particular person, who may also have other characteristics, such as political affiliations, or disabilities, that they would prefer not to reveal.

Unfortunately, under the standard, such attribute certificates are intrinsically linked ('hierarchical children of') the identity certificate. So with contemporary PKI a person has to declare their identity first, in order to declare a credential or eligibility.

So while it is possible to allow people to have attribute certificates divorced superficially from their identity, this identity is always known at least to the Registration Authority. Placing a digital signature certificate on an ID card which also displays the 'distinguished name' immediately negates this 'pseudonymous' option.

Both the existing and proposed ID Card schemes include absolute requirements in relation to identification, the use of a single pair of identifiers (card-number and registered name), and requires registration of aliases. There is therefore little scope in Hong Kong for the use of PETs which encourage anonymous or pseudonymous transactions. Changes to the law would be required which would not be consistent with current policy.

Analysis of Privacy Principles

This section of the PIA will include consideration of current and future compliance with the Personal Data (Privacy) Ordinance. For the purposes of this analysis, we make the assumption that ImmD is and will remain the primary data user in respect of both the ROP database and other ROP records. In addition we take the view that in the current system, ImmD is also the data user, or at least a data user, for all of the data displayed on the HK ID Card, bearing in mind that the cards are issued to and held by individuals who exercise some control over the use of the data concerned. This means that ImmD is responsible for setting the terms of the uses

and disclosures of the card information, within the framework of the relevant Ordinances. The Privacy Commissioner's *Code of Practice on the Identity Card Number and other Personal Identifiers* does not detract from this responsibility as it simply explains the position and how the Data Protection Principles apply to the collection, use, etc. of the number on the HK ID Card.

Responsibility for compliance with the Personal Data (Privacy) Ordinance will potentially become more dispersed and confused if the new card is to be used for new applications unrelated to immigration matters. This will also be the case if administration of even limited aspects of card administration are transferred to another agency, as is apparently under consideration. It is not sufficient to say that each agency implementing an application on the card will be responsible for its own data - there will clearly be common data, and there must be clear and unambiguous responsibility for the overall parameters of card design and use. Otherwise, the risk of uncontrolled 'function creep' will be that much greater.

It is recognized that ImmD receives very few enquiries or complaints from the public about privacy and related issues. There have also been very few complaints to the Privacy Commissioner for Personal Data about ImmD compliance with the Personal Data (Privacy) Ordinance.

There must be clear and unambiguous responsibility for compliance with the Personal Data (Privacy) Ordinance in relation to the HKSAR ID Card and all data held in connection with registration and operation of the Card.

Collection

The personal information that ImmD collects about individuals under the ROP Ordinance for the purposes of registration, which will not change in the new system, can generally be justified as necessary for ImmD's purposes, and such collection is also both fair and lawful, as required by DPP1.

Statutory amendments will be required to the ROP Ordinance and Regulations to provide for the new scheme[33], including specifically for the taking of a second thumbprint (ROP Reg 4);

It needs to be recognised that data items that may appear mundane to many people can be especially sensitive to some individuals, in particular residential address and telephone, but also name and telephone of school/company, marital status, spouse's name and card-number, and profession/occupation.

ImmD includes a statement of purpose on all its application and notification of changes forms, designed to meet the relevant requirements of DPP 1(3), which requires data subjects to be informed of a range of matters. The statement appears to cover most of these matters adequately, but three items are not as clear as they might be:

- "any other legitimate purposes" (1(h)) in the list of proposed uses) is arguably too open-ended to satisfy the requirement to inform the data subject of the purpose for which the data will be used. On the other hand, if this means "where required

[33] See Feasibility Study Report, Part 1, Section 8.

or authorized by law" (including in the circumstances permitted under ss.57-59 of the Personal Data (Privacy) Ordinance), then it would be clearer to say this;

- "for statistics and research purposes" (1(g)) is also a little ambiguous. The PDPO s.62 provides an exemption from DPP3 (the use restriction principle) for statistics and research, but on condition that the results are not made available in a form which identifies any data subjects. It is not clear if this item is intended to cover research uses of this sort and/or to provide for other research uses that involve identification of subjects;
- "…to assist in the enforcement of any other Ordinances and Regulations by other government departments through carrying out immigration control duties;" (1(e)) is also unclear, in that it is not clear if it covers only assistance provided incidentally to the conduct of immigration control, or if it extends to assistance requested by other departments and agencies, using immigration control facilities and resources, including ROP data. This item has the further difficulty that it may be inconsistent with the requirement of DPP1(1)(a) that a data user may collect personal data only for a purpose that is necessary for or directly related to a function or activity or the data user.

These may seem narrow technical points, but are significant given the objective of DPP1(3) which is to inform individuals how personal data collected from them is to be used. This will become of increasing importance if the uses of the HKSAR ID card are to be wider than those of the existing HK ID Card, as is proposed. Either 1(d), 1(e) or 1(h) in the statement of purpose must cover the uses, including disclosures, to other government agencies, apart from the High Court and the REO which are expressly named.

ImmD will need to ensure that the statement of purpose and of the parties to whom the personal data may be transferred (DPP1(3)(b)(i)(B)) keeps pace with the actual uses and disclosures of personal data, both now and particularly under the new system. It would for instance be helpful to expressly mention disclosure to the HK Police, as they are already such major and significant users of ROP data, and may well become more so as more data becomes available electronically in the new system.

ImmD should review the adequacy and accuracy of its 'statement of purpose' included on forms to satisfy the underlying objective of DPP 1(3), addressing the issues raised above and any others revealed by the review.

ImmD maintains that even if it is decided to use the new HKSAR ID Card for other applications, there will be no further transfers of registration data between ImmD and the agencies responsible for, or using, those applications. ImmD has consistently taken the view that other applications will not be allowed to affect the registration process, including the amount and type of information requested, which will remain determined solely by ImmD needs. Maintaining this commitment will be important to prevent function creep. A consequence of allowing any departure would be a potential conflict with the requirement of DPP1(1)(a) on a data user to collect personal data only for a purpose that is directly related to one of its functions or activities. In addition, adequately explaining on who's behalf personal data is being collected, and how it is to be used, to comply with DPP 1(3) could become a significant challenge.

ImmD may wish to consider whether arrangements can be made, and facilities provided, for a range of individuals who have special circumstances or needs. These include, potentially:

- persons-at-risk (various categories described above under Special Arrangements);
- public figures, whose participation in normal registration processes might cause difficulties either for them or for ROP staff; and
- Persons with genuine objections to the standard processes for capturing photograph or thumbprints, either for religious or conscientious reasons or because of disfigurement.

Special arrangements or facilities could include:

- private booths in registration offices;
- alternative locations for registration;
- additional ID Cards;
- non-recording of certain data;
- approved recording of alternative details;
- suppression of certain details on the ROP database; and/or additional access controls.

Data quality

The requirement of DPP 2 to keep personal data accurate is qualified - it only needs to be accurate 'having regard to the purpose (or any directly related purpose) for which the data are or are to be used'. This qualification is very significant, as it prevents this principle becoming a major 'driver' for requiring individuals to notify changes to their registered particulars. The fact that the current system appears to work adequately notwithstanding the low level of enforcement of changes notification suggests that the data is 'sufficently' accurate to serve its intended purposes. However, it is understood that the absence of enforcement has more to do with lack of resources than a positive policy decision, and that ImmD would ideally like to maintain an up-to-date population register with current contact and location details for all individuals. This would have advantages for some of ImmD's functions which involve contacting relatives, but it would dramatically change the nature, and value to other agencies, of the ROP information.

ImmD needs to review the need for the items of information required under ROP Regulation 4 to be updated. If the only reason for requiring individuals to notify changes is to meet the needs of other agencies (such as the REO and High Court), and there is no ImmD need, then the question arises as to whether ImmD can comply with DPP1(1)(a). If on the other hand ImmD can demonstrate how updated details assist in one of its functions or activities, then this part of the Principle would be satisfied.

Another potential source of inaccuracy is the misallocation of details within the ROP systems, either by mis-keying, corruption in processing. or in other ways. ImmD

systems are designed to minimize these errors, largely at present through multiple manual/visual checks. The new system will include additional automated processes, specifically auto-comparison of old and new thumbprints. While this will be more efficient and reduce the potential for human error, it is important that logical checks are built in and that users of the data are informed about the likely level and types of error that may remain (in general terms). This will be necessary to avoid individuals being put under suspicion, or challenged, as a result of discrepancies which could arise from systems error.

Consideration should also be given to statutory amendments to give legal protection to individuals against 'presumption of guilt' due solely to technology failures (eg: corrupt or damaged cards, card-receiver failure, loss of communications links).

ImmD should review its records retention policy and develop and implement a disposals schedule in respect of all personal data, in all storage media, to comply with the requirements of DPP 2(2) and s.26 in relation to retention and erasure of data when the purpose for holding it has expired.

Use and *Disclosure*

Uses and disclosures of personal data from the HK ID Card and from the ROP database and microfilm records are currently governed mainly by DPP 3 of the Personal Data (Privacy) Ordinance, the Registration of Persons Ordinance and its Regulations, and Part IV of the Immigration Ordinance. There are also a variety of specific provisions in other Ordinances or subsidiary legislation (such as the Jury and the Electoral Affairs Commission Ordinances) that sanction the disclosure of ROP information for particular purposes. ImmD issued internal guidance on compliance with DPP 3 in 1996 (in relation to disclosure or transfer between departments - IDC No 44/96); and in 1997 (in relation to public consultation exercises - IDN No 262/97).

In relation to use of the card and card number, there are some mandatory uses, specified in law, and other uses which are effectively mandatory because of a requirement to provide evidence of identity (the only alternative accepted being a HK passport which not everyone has). However, there is no legal constraint on the circumstances in which any person or organization can request an individual to show their HK ID Card, the only limits being on the copying of cards and recording of the HK ID Card Number, imposed by the Privacy Commissioner's *Code of Practice on the Identity Card Number and other Personal Identifiers.*

Statutory amendments will be required to the ROP Ordinance and Regulations, and possibly to other laws, to provide for the new scheme[34], including specifically for the following elements:

- reading of 'non-visible' card data by agencies other than ImmD (such as the HK Police);
- provision of thumbprints (to ImmD and others agencies) in various scenarios where the HK ID Card is currently required to be shown, for comparison with the prints recorded in digital form on the card.

[34] See Feasibility Study Report, Part 1, Section 8.

The following suggestions are made in the light of the above and the Legal Analysis in Part IV.

ImmD should ensure that all disclosures from the ROP database and other records (whether provided directly or via an ability to read card data) are authorized by relevant permission under ROP Regulation 24, where this is required.

ROP Regulation 24 should be amended to expressly cover all personal data held by ImmD in connection with the ROP function. Consideration should also be given to moving the prohibition into the ROP Ordinance itself, or any amendments made subject to the express approval of LegCo (i.e. positive disallowance), so that it cannot be overridden by pre-existing provisions in Ordinances giving a power to obtain information. Further, any subsequent legislative provisions to authorize disclosures of ROP information should also be subject to a positive approval process in LegCo.

The ROP Ordinance should make *all* unauthorized use (including 'mere' browsing), and including unauthorized disclosure of the information concerned, an offence, subject to suitable penalties

The Personal Data (Privacy) Ordinance contains special provisions relating to matching procedures[35], which are a particular type of automated matching of personal data. The relevant part of the Ordinance was commenced in 1997 and requires Privacy Commissioner approval for any matching procedure. ImmD issued internal guidance on these provisions in IDN No 282/97. The only matching procedure for which ROP data is currently used is the comparison of data with the REO for electoral registration validation. The Privacy Commissioner issued an approval for this procedure in 1997[36]. ImmD will need to ensure that any requests for further automated matching that meets the definition of matching procedure in the Ordinance which may be made once the new system is operational are submitted to the Privacy Commissioner for approval. Any agency considering making such a request should be aware that approval is not automatic or guaranteed, and that the Commissioner may consult with other interested parties, and may impose conditions.

Another use of the information collected in registration is to personalize the ID card itself. The proposed reduction in personal data appearing on the face of the card is a privacy-positive feature.

Privacy concerns about the use of personal data held on, or supplied in connection with, the HKSAR ID Card would be significantly reduced if ImmD, or the government as a whole, were able to give commitments:

- that the card will not be contactless;
- that the details which are permitted to be displayed on the card will be no more than those envisaged in the Feasibility Study Report;
- about the specific data items that may be stored in the chip;

[35] Personal Data (Privacy) Ordinance, Part IV - ss.30-32.
[36] Approval of Request No 19970708087 (from the Electoral Affairs Commission, REO), 24 October 1987

- about the organizations or classes of organizations permitted to access data directly from the chip, and for what purposes;
- about the organizations or classes of organizations permitted to take (or read) thumbprints for the purpose of comparison with the digitized print on the card,and the circumstances in which this will be permitted. Specifically, the grounds under which the taking of thumbprints by the HK Police, and any other secondary users of the system in this way, should be prescribed in detail; and
- about the circumstances under which conversion of any of the information which is merely imaged (previously microfilmed) into fully machine-readable form is permitted

Person-to-person linkage is a very privacy-invasive activity; i.e. extracting data about an individual solely because of their connection to another individual of interest, without any prior suspicion or evidence that the associated person is also of interest. In the ROP database, associations would typically be in the nature of family relationships e.g. parent-child, guardian-child, spouses.

ImmD should ensure that provision of 'associated person' data, in response to enquiries from authorized agencies, is covered by proper legal authority; i.e. that permissions issued pursuant to ROP Regulation 24 are worded so as to allow ‘associated person’ data to be disclosed.

Security

DPP 4 requires agencies to take all practicable steps to protect personal data against unauthorized or accidental access, processing, erasure or other use, having regard to specified factors. Security issues are fundamental and have been addressed in the Specific Privacy Implications section above.

The data stored on the Card chip for the ROP/ID Card application should be subject to all of the limitations embodied in the Feasibility Study Report, in particular:

- that they are limited to the data-items currently envisaged and set out in that Report; and
- that they are subject to the specified technical protections;
- that they are accessible only by the specified and very limited number of devices and organizations for the specific purposes stated

The design specification for the new system should expressly include the following:

- the card-number should continue to convey no more information about the cardholder than it currently does;
- segregation between and independence of the functions that the card performs ;
- standards to ensure that no application will be able to compromise any other applications or their associated data; and
- technical features that prevent access to data and functions where no legal authority exists for linkage.

The Request For Tenders should explicitly require proposals to explain precisely how integrity of data and functions will be protected, and the details of relevant:

- hardware features;
- systems software features; and
- application-level features.

The card should perform challenge to and authentication of devices and processes with which it interacts, and only participate in processes where the results are satisfactory, in order to provide protection of the data against disclosure to, and of processes from performance by, unauthorised parties.

The card should participate effectively in the authentication of the person presenting it, in order that the card prevents the exercising of the cardholder's prerogatives by an imposter.

It is highly desirable that the biometrics stored on the card do not leave the card under any circumstances. To achieve this, the comparison between a newly captured thumbprint and that stored on the card would need to be performed by the chip on the card, and not by the card-receiving device. The security level would need to be comparable to that of secure PIN-pads in financial services applications. It is uncertain whether the technology is currently available to perform this function on the card.

The request for tender should invite tenderers to address this issue. It should be made a 'highly desirable' feature that would weigh significantly in the assessment of tenders, if it proves to be available.

If the cards are to be capable of supporting cryptographic functions, then the following additional specifications should be included:

- the card must perform secure key-generation, and provide secure key-storage, and secure key usage for both digital signature and message-encryption key-pairs;
- cardholders must be given the choice concerning how many key-pairs, and how many certificates are acquired, and which are used under what circumstances;
- any backup arrangements for private keys need to be entirely at the discretion of the cardholder, such that individuals have a genuine choice of organizations offering back up services, including non-government service providers;
- if the private keys are stored elsewhere other than on the chip, no government agency should be able to gain access to any such backup; and
- compulsory escrow arrangements for private keys must be precluded.

Privacy concerns would be eased if ImmD could confirm that the digital thumbprint will only be used for one-to-one comparisons for the purpose of authenticating the identity of a person, and for no other purpose, especially for one-to-many comparisons in order to identify a person from their thumbprints.

ImmD should:

- design alternative processes and procedures to handle a situation in which thumbprints are not held on the ROP database, or are held only in template form;
- in the Request For Tender, require tenderers to provide proposals relating to alternative implementations in which the ROP database contains the thumbprint, contains only a template of the thumbprint, and contains neither;
- conduct trials to confirm that these procedures do not significantly reduce the integrity of the scheme, nor unduly increase the efforts and costs of individuals or the ROP Registration Office;
- subject to satisfactory outcomes of these trials, implement the system without storing the thumbprint in the ROP database.

An appropriately qualified independent technical consultant, should certify, following a technical audit, that the design and implementation of the scheme ensures that the following risks have been comprehensively and effectively addressed:

- the risk that the card might be used to store data that is unknown to the person, may be against the person's wishes, and/or may be harmful to the person's interests;
- the risk that the card might be used to disclose data in a manner that is unknown to the person, may be against the person's wishes, and/or may be harmful to the person's interests;
- the risk that the card might be used to perform functions, and/or to participate in the performance of functions that are unknown to the person, may be against the person's wishes, and/or may be harmful to the person's interests;

and, if the key is to support cryptographic functions:

- the risk that a private key could be discovered; and
- the risk that a private key could be invoked by a person other than the cardholder, to digitally sign outgoing messages and/or to decrypt incoming messages;

and, in relation to card-reading devices:

- the risk of interception of traffic, and hence access to personal data or access to a stream of data that can be replayed later as a means of achieving masquerade. This risk is present:
    - within the device;
    - between the device and the card; and
    - between the device and any other device with which it communicates, such as a local server, or a remote server by means of a communications router;
- the risk of the recorded biometric becoming capturable by other agencies, organisations or individuals. This can arise if the biometric is not adequately protected, e.g. because it is not encrypted, or the hashing algorithm is not one-way, or the compression is insufficiently 'lossy' and hence the compressed form can be used to generate an adequate masquerade;
- the increased risk of other organisations seeking to capture the biometric themselves, as a more efficient means of authentication than visual inspection of the ID Card;

- the increased risk of the recorded biometrics being obtained illicitly and used by imposters to masquerade as an individual, e.g. as a tool for 'framing', by leaving latent prints at the scene of a crime;
- the risk of the PIN or PINs being captured;
- the risk of masquerade use of unsupervised devices (such as self-service kiosks) by imposters who acquire the card and any necessary knowledge such as a PIN, and/or are able to simulate the biometric; and
- the risk of card-data being amended by inappropriate devices, e.g. at ImmD control-points rather than ImmD Permits and Visa, or by any other organisation that installed equivalent devices.

The new scheme should embody all of the privacy-positive security features that are in the existing scheme, including access controls and interface controls relating to other ImmD systems, and external systems such as ECACCS, and ensure that they are applied at all times, including, for example, to temporary and mobile registration operations.

ImmD should work towards integrating access controls to its computer systems with its human resource management system(s), in relation to the timely invalidation of user ID/password pairs on departure of staff and during extended periods of absence.

The specifications of the scheme relating to the gathering of logs and audit trails should be enhanced to ensure that sufficient detail is gathered that anomalies can be detected, investigations undertaken, and miscreants identified, and that the procedures and processes are actually performed, and that identifiable anomalies are in practice identified.

Privacy intrusion will be affected, at least potentially, by the far greater reliance of the new scheme on technology in general, and the electricity supply, networks, computers, cards and chips in particular. Malfunction and unreliability of services will not only cause considerable inconvenience but may also result in individuals being wrongly suspected or detained in error.

The specifications for the scheme should be amended to require much higher standards of reliability and resilience than the "at least that of the current system" suggested in the Feasibility Study Report, and disaster recovery planning should be based on much more than the suggested 'minimalism' implying only 'basic survival' mode.

ImmD should include understanding of the privacy issues associated with ID cards and their use, and the way in which these issues have been addressed, in training programs for relevant staff.

Consideration should be given to the following additional statutory amendments to support the technical and organizational security measures:

- making it an offence to solicit (with or without payment) unauthorized disclosure of ROP data;

- placing limits and/or conditions on the use of ROP data by persons or organizations to whom ROP data is disclosed (both directly pursuant to ROP Regulation 24 and indirectly under Regulation 23), and making it an offence to breach those limits/conditions.

ImmD should re-affirm its commitment to take disciplinary action against any officers or employees breaching security, and/or using personal data outside relevant legal authorities.

Openness & Transparency

As a general matter, the privacy principles adopted around the world, including the DPPs in the Personal Data (Privacy) Ordinance, all emphasise openness and transparency (see DPPs 5 and 1(3)), and one of the best ways of disarming unwarranted suspicions about 'function creep' is to be open about the extent of data sharing. Publication of aggregate statistics about disclosures of ROP information to other agencies would be a significant demonstration of commitment to this principle. It would also be likely to rebut uninformed and exaggerated speculation about the extent of data sharing.

The uncertainty over what, if any, additional applications will be installed on the new card also makes it difficult to comply fully with the spirit of DPP 5. While it may be factually correct to claim that decisions about other applications are outside the control of ImmD, the fact that the specification for the new card may include provision for other, as yet unspecified, applications will invite speculation. Unless certain applications and functionality are ruled out, the Hong Kong public are entitled to assume that anything is possible, and base their reaction to the new card on the widest possible range of different uses and purposes.

It is partly in the spirit of the openness and transparency principle that Privacy Impact Assessments should be carried out in public, and with the widest possible input. While there has been no public input into this PIA to date, public release of the PIA report as soon as possible would be consistent with the objective of DPP 5 of the PDPO.

Consultation

Wider consultation about the HKSAR ID Card scheme would both engender confidence in the scheme, and enable ImmD to take account of any concerns in the design. Wider consultation would provide an opportunity to assess the strength of the potential concerns identified in this report, and wherever possible address or otherwise accommodate them. The information made available as a basis for consultation would also serve to disarm uninformed criticism of the scheme on the basis of features which are not intended and may indeed have been ruled out.

ImmD has already undertaken consultation with a range of government agencies, including:

- the Hong Kong Police;
- the Registration and Electoral Office;
- the Registrar of the High Court; and
- other government users of the current HK ID Card.

To date, public consultation has mainly comprised briefings given to the LegCo Security Panel and the Privacy Commissioner's Committee on Technological Development. Ideally, the public consultation process should explain to the general public, as the ultimate stakeholders, both the benefits of the scheme and the privacy implications and issues (and other 'consumer' implications), and provide a meaningful opportunity for public feedback to be taken into account. It is acknowledged that ImmD's timetable places constraints on the process. Nevertheless, it should still be possible to take the following steps:

- Ideally, this PIA should be made public, to assist consideration of the proposal by legislators and other stakeholders.
- In order to facilitate understanding amongst stakeholders, ImmD should make available technical briefing materials. The Historical Background and Overview in sections 5.1-5.3 of the Market Research Report of April 2000 (pp.50-67) would be a valuable tutorial for interested parties.
- In addition to public release of the PIA, it should be given to key representatives of the public.
- Given the tight timetable, ImmD could consider convening a public interest reference group, comprising key representatives, to provide an efficient channel for information about the proposal, and for feedback.

Most of the public interest can be expected to focus on uses of the scheme and on the legislative framework and safeguards, rather than on technical design issues. The legislative and organizational aspects have a longer time frame for decisions than the technical specifications. Consultation would not therefore need to be completed in the immediate future and could proceed in parallel with the tendering process

Research into Public Attitudes

In the section above on Public Attitude Analysis, the lack of knowledge of the views of Hong Kong's population about ID Cards was emphasized. The single question about the use of the ID Card Number asked in the Privacy Commissioner's annual surveys from 1997 to 1999 gives the only clues to these views[37].

The decision making process would be much better informed if at least some professional research was conducted. This need not take the form of elaborate and expensive quantitative surveys or polling, although quantitative findings would be helpful. Well-designed qualitative research, using focus groups, would establish the range of attitudes and opinions about both the existing ID Card and the proposed new card system and its uses.

The results of any such research would be a valuable resource for public debate.

Public Information – awareness, education and training

[37] Results of the 2000 survey are expected to be published later in September.

Given that the new HKSAR ID Card scheme will inevitably raise privacy concerns, it is very important that adequate attention is paid to privacy issues during the implementation of the scheme.

There will presumably be a major public information and education campaign prior to the commencement of re-registration; and there will also need to be awareness and training activity associated with the proposed 'kiosks' at which individuals will be able to check the contents of their cards. Explanation of privacy issues and the ways in which they have been addressed should form part of these campaigns.

ImmD should incorporate material on privacy issues into public information campaigns and related activity preceding and accompanying the introduction of the new ID Card.

Access & Correction

Another fundamental privacy principle is the right of individuals to see what information is held about them and to correct it if it is wrong. In Hong Kong, this is given effect by Data Protection Principle 6 and Part V of the Personal Data (Privacy) Ordinance. The right of access is provided for by s.18(1)(a) of the Ordinance, subject to a range of exemptions set out in Part VIII, while s.22 provides for a right to request correction of personal data supplied pursuant to an access request.

ImmD has issued guidance within the Department about compliance with these access and correction provisions. Early notice of these provisions was given as part of the general guidance on introduction of the PDPO in IDC 45/96. This has been followed by specific advice on log books for refusals to comply with data access requests (IDN 319/98); on the 40-day time limit for compliance with data access requests (IDN 213/99), and on the introduction of the data access request form specified by the Privacy Commissioner under s.67 of the Ordinance (IDN 338/99).

ImmD's approach to satisfying requests for access is to use existing statutory processes where they already exist. This means that in respect of ROP data, individuals are required to apply for a Certificate of Registered Particulars pursuant to ROP Regulation 23, using Form ROP 122, and paying a fee of $395. Most of the template certificates used in reply to such applications are designed to meet the particular needs of third parties requiring individuals to obtain a certificate in the context of specific transactions (eg: application for emigration, certification of address or marital status). There is however one standard purpose - certification of all particulars on record, which would presumably be nominated by individuals whose motivation was purely to exercise their PDPO rights. ImmD needs to ensure that responses to these requests satisfy DPP 6 and s.19(1) by providing all of the applicable personal data, together with whatever explanation may be required (eg of codes).

ImmD should review its processes for responding to subject access requests under DPP 6 to ensure that individuals are given access to all the ROP data to which they are entitled.

Compliance with the access requirement will become in some ways easier and in other ways more difficult with the advent of the new HKSAR ID Card system. Easier

because all supporting documentation will be digitized and more easily retrievable. More difficult because, in addition to the database information, ImmD will need to explain what information is actually held on the smart card itself.

The Feasibility Study Report proposed that ImmD should provide public kiosks where individuals could check the contents of their own card. Leaving aside issues of security already discussed, it seems clear that self service kiosks should be seen as a complement to, rather than as a replacement for, a more formal data access request process. Apart from any other consideration, as they will not be fitted with printers, the PDPO requirement to provide a copy of personal data requested pursuant to a data access request would not be met. Formal data access requests will therefore need to be dealt with, as now, by a separate process.

Privacy Impact Assessments

The Feasibility Study Report, and the request for tender for this PIA, anticipated 3 further PIAs at later stages of the project.

In addition to further PIAs, it is important that the RFT should be formally reviewed, prior to despatch to vendors, by persons with specialist expertise in the privacy aspects of schemes of this nature, to ensure that any additional privacy-positive measures adopted as a result of this PIA Report have been translated effectively into tender specifications.

Further, the selected tender should be reviewed, prior to finalisation of the contract, by persons with specialist expertise in the privacy aspects of schemes of this nature, for its conformity with the privacy requirements of the RFT.

PART VI – CONCLUSIONS

Conclusions

In Hong Kong, the existing ID Card, and its widespread use in both public and private sectors, appears to have been accepted without major concern. The privacy-intrusive potential of the Card has however been limited by several factors; notably the lack of easy access to registration information, and the fact that the information is generally not kept up to date.

The Immigration Department's proposals for the new HKSAR ID Card, in relation to its own functions and activities, are modest and do not involve significant new uses. Nevertheless, several aspects of the proposed new Card and its supporting infrastructure have significant privacy implications. The use of a smartcard with 'invisible' data, the inclusion of a digitized biometric (thumbprint) and the consequent use of card receiving devices all change the nature of the scheme in ways which some people will see as threatening to privacy. In the consultants' judgement, the easier access to 'imaged' registration data is also likely to lead to greater use of that information by other agencies, which in turn could lead to pressure on ImmD to maintain a more up-to-date population register. Such a development would be very significant in privacy terms.

If the new HKSAR ID Card is designed to support other applications, even if those applications have yet to be decided, then a range of other privacy issues arises. While there is uncertainty about what other applications might be added to the card, there will be a level of concern about the potential of the Card to lead to an increase in the degree of monitoring, surveillance and data linkage – all of which are significant privacy issues.

Resolution of privacy issues arising from the HKSAR ID Card project can be approached from two different perspectives:

- Seeking to minimize any adverse privacy impacts;
- Seeking to minimize the risk to the project from failure to adequately address privacy concerns.

As far as possible, the conclusions and suggestions in this PIA have aimed to meet both objectives.

The conclusions and suggestions can also be categorized in a number of different ways:

- Whether they are endorsements of decisions already made, or will require new decisions;
- Whether they can be acted on by ImmD alone or need to be addressed at a whole-of-government level;

- Whether they are time critical in relation to the tendering process, or can be addressed in parallel with that process;
- Whether they relate to:
    - technical design issues
    - legal compliance issues
    - management of public perceptions

ImmD has already shown a good understanding of many of the privacy issues, particularly those concerning security and confidentiality of data, and compliance with the Personal Data (Privacy) Ordinance. Some of the decisions that have already been taken, such as not to specify a contactless card, and not to convert some application details into machine-readable form, are strongly privacy-positive.

It is clear that ImmD's current intentions are that the HKSAR Card scheme should largely be a straightforward technological update of the existing Card scheme, with only marginal changes to functionality, registration requirements, uses and permitted disclosures of information. In this respect the scheme design is re-assuring and privacy-positive.

The main privacy risks relate to the potential for the new Card to lead to greater use by a range of other government agencies, and possibly by non-government organizations including businesses. The ease of use of a smart card, and the significantly enhanced ability to access imaged data as compared to the existing microfilm records, may lead to increased incidence and frequency of card inspection, increased demand for access to ROP information, and even demand for additional information collection during registration.

ImmD is constrained in its ability to address the significant privacy issues by the fact that decisions about other applications are being made in a wider whole-of-government context. However, the fact that the decision appears to have already been made to facilitate other applications, as yet unspecified, means that ImmD cannot avoid having to address all of the privacy issues raised by that decision.

By specifying an infrastructure which can support other applications, the HKSAR ID Card project becomes at least a whole-of-government (and perhaps wider) initiative. The Registration of Persons function necessarily becomes one which at least potentially supports other card applications and uses, and which must therefore be regarded as potentially subject to alteration to meet the needs of other agencies.

Unless the government is prepared to expressly rule out certain other applications and uses, there will inevitably be a public perception, in some quarters, that the HKSAR ID Card is at least potentially the first step towards a more comprehensive population registration system that would support an increased level of monitoring and surveillance.

Overall Privacy Strategy

ImmD needs to recognise the very substantial privacy implications of the proposed scheme, and the resultant need for an integrated strategy in relation to all of the following:

- legal authorisations and constraints;
- consultation, preferably directly with the public, but at least with key representatives;
- technical specifications;
- organizational policy commitments;
- compliance with the Personal Data (Privacy) Ordinance; and
- public awareness, education and training campaigns.

Implementation of an integrated privacy strategy will involve a combination of legislative amendments, policy commitments, and specifications in the scheme design, tendering, contractual and implementation stages of the project.

PART VII – APPENDICES

1. Pacific Privacy Pty Ltd and ImmD Staff involved

2. Letters to ImmD from the Privacy Commissioner for Personal Data

3. Data Privacy and Security Recommendations from the Feasibility Study Report

4. Meetings with Stakeholders

5. International Experience

6. Bibliography & other resources

APPENDIX 1
PROJECT PERSONNEL

Pacific Privacy Pty Ltd

Mr Nigel Waters

Managing Director, Pacific Privacy Pty Ltd, Nelson Bay, NSW, Australia.

Formerly Deputy Federal Privacy Commissioner, Australia, and Assistant Data Protection Registrar, UK.

Dr Roger Clarke

Associate. Privacy, Information Technology and E-commerce consultant, Formerly senior academic in Information Systems, Australian National University.

Mr Robin McLeish,

Associate. Barrister-at-law, Hong Kong. Formerly Deputy Privacy Commissioner for Personal Data, Hong Kong, and Principal Assistant Secretary, Home Affairs Bureau.

Ms Lindy Smith

Associate. Privacy consultant. Formerly Director of Policy, Office of the Federal Privacy Commissioner, Sydney, Australia.

Ms Sue Grdovic

Associate. Formerly Director, Promotion and Education, Office of the Federal Privacy Commissioner, Sydney.

* * *

Pacific Privacy acknowledges the assistance of staff in the Special Assignments Section, the Registration of Persons Sub-division and the Information Systems (Production) Division of the Immigration Department.

.

APPENDIX 2

EXTRACT FROM INFORMATION PAPER FOR LEGCO SECURITY PANEL MEETING, 1 JUNE 2000.

(Progress Report on the HKSAR Identity Card Project)

Data Privacy and Security

7. On data privacy and security, Consultants recommended that the design of the new ID card and the new computer system must have regard to the following issues: -

(a) Compliance with the Personal Data (Privacy) Ordinance;
(b) Designing systems and procedures in a privacy-sensitive manner; and
(c) Use of Privacy enhancing technologies to prevent identity theft and to protect the data privacy of the individual.

8. More specifically, Consultants recommended that the following data protection measures should be adopted: -

(a) Protection of data on the card (e.g. biometric data, personal data) against unauthorised access by means of access controls enforced by the card itself, so as to ensure that any request to read the data coming from an unauthorised system will not be entertained;
(b) Protection of data in ImmD systems by means of system access controls that are well-tested, including passwords, different levels of authority and audit trails;
(c) Strong enforcement of access controls on sensitive data, including biometric data, by encryption of the data stored on cards, in computer systems, and during transmission within and between ImmD offices. Even if encrypted data are intercepted by an unauthorized person, they will be in the form of a set of meaningless characters and numbers;
(d) Data may be encrypted in such a way that separate keys are used for each type of data and for each card, so that staff of different departments or if necessary, different staff within the same department, can only have access to those data as are relevant to their scope of work;
(e) Use of tamper-resistant hardware security devices (which will stop functioning if it detects that several unsuccessful attempts have been made to read the data on the card or to gain access control to

the system) to strongly protect the cryptographic security of the systems;

(f) Protection of data on the card from fraudulent changes by using cryptographic data integrity so that fraudulent data or fraudulent cards cannot be created;

(g) Provision of self-service kiosks in ImmD offices so that cardholders can view the data on their cards, using biometrics for access control (the card will also check the authenticity of the kiosk before releasing the data);

(h) There will be no facilitation of one-to-many matching of biometric data, which means that the biometric data will be used only for the purpose of authenticating a named person's identity card and it will not be possible to use the data to search the entire database for a match; and

(i) If the identity card is to used for multiple purposes, using smart card and a smart card scheme that guarantees separation of uses from each other, so that immigration data on a card will be protected from access by other departments and vice versa.

APPENDIX 3

TWO LETTERS FROM THE PRIVACY COMMISSIONER FOR PERSONAL DATA TO IMMD CONCERNING THE HKSAR ID CARD PROJECT

Our Ref: PCO/1/150/3

15 March 2000 (by hand)

Mr T P Wong
Deputy Director (Special Assignment)
Immigration Department
23rd Floor, Immigration Tower
7 Gloucester Road
Wanchai, Hong Kong

Dear Mr Wong

Re: New Identity Card

With the feasibility study currently being conducted on the introduction of a new Identity Card, I have recently been approached by many including the media on my views on this Government initiative. While I fully appreciate the reasons and rationale for this Card to be a smart card with multi-applications capabilities, I have expressed considerable reservations with regard to the potential dangers of privacy invasion. I therefore believe it is relevant to communicate my views at this point in time to the Government for consideration in the current feasibility study. Obviously when the feasibility report is available in the near future, I will be in a better position to have more specific views on the matter.

The new ID Card, as I understand it, will serve not only to identify the individual, but also to have value-added applications to be built in the Card to enhance efficiency of government services as well as to provide benefits, such as convenience and access, to the community. It is therefore expected for the card to contain substantial amount of personal data, e.g. personal particulars including biometric attributes to uniquely identify the individual, and other personal data required to support the various applications. With such concentration of personal data, some deemed to be sensitive, on a single card, potential problems of data privacy can be perceived:

IDENTIFY THEFT

In this information age, with increasing automation and less and less face-to-face contact for service application and delivery, business practices and their underlying technology tend to regard whoever presenting the Card at the card-reading terminal as the true owner of the card.

- 2 -

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. Whether justified, whether righteous, the net effect is an undeniable 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 A **Privacy Impact Assessment (PIA)** should be conducted in the planning stage. 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 attach, in Appendix A, a paper for your reference, "Privacy Impact Assessment: Towards A Better Informed Process for Evaluating Privacy Issues Arising from New Technologies, Such as Biometric Identification" (1998)

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 have the right to participate in the determination of what personal data the card contains and who has access to it.*

Informed Consent *All additional uses and disclosure of information should be subject to the prior and informed consent of the citizens.*

Informed Choice *Where possible, the citizens should be free to choose the applications on offer. In other words, subscription to the applications should be voluntary.*

- 3 -

Non-discrimination *The information on the Card should as consented to by the citizen concerned 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 card holders 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. I firmly believe the Government should consider **the use of biometrics together with privacy enhancing technology (PET)** to prevent identity theft and more importantly to protect the privacy of the individual from secondary uses of his personal data without his consent or involvement. I attach two documents (Appendix B and C) which go into significant details of biometrics and PET.

- "At face value - On biometrical identification and privacy", Registrateikamer, the Hague (The Netherlands Data Protection Authority), September 1999

- "Biometric Encryption - New Developments in Biometrics", Dr George Tomko, September, 1996

These reports offer guidance on how these technologies can be applied in ways that do not infringe individuals' privacy. In particular, the Netherlands Report makes several recommendations on how best to avoid privacy risks when using biometric technologies, for example, encryption of databases where personal data is being stored.

4. It is also 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. While arguably there will be departure or exemptions from these principles on the basis of public interest, the administration code should establish precise conditions upon which such exemptions could be exercised, with checks and balances to minimize inadvertent or otherwise the violation of the rights of the citizens.

I am grateful if my views are made known to the working party and the consultants involved with the feasibility study, and I am happy and willing to provide any assistance to their work if you so wish. I firmly believe that with the right objectives, design, security and community education the Government will be able to implement a new ID Card system for the benefits of our community while at the same time safeguarding the right to privacy of our citizens.

Yours sincerely

Stephen Lau
Privacy Commissioner for Personal Data

cc Mr Ng Hon Wah, HAB

Encl.

PC/sps/U:kitty/kcmisc2.doc

Our Ref: PCO/1/150/3

28 July 2000 (by post)

Mr T P Wong
Deputy Director (Special Assignment)
Immigration Department
23rd Floor, Immigration Tower
7 Gloucester Road
Wanchai, Hong Kong

Dear Mr Wong

Once again, I thank you and your colleague Ms Helen Wong for the informative presentation on the new I.D. Card project to our Office's Standing Committee on Technological Development earlier this month. For the record and for your consideration, I wish to reaffirm the major observations of the Committee members in the Committee meeting:

1. The members have serious reservations with regard to the potential privacy invasion in the use of the new I.D. Card, other than for Immigration Department purposes, by other Government departments and the private sector. It is not a matter of primary concern with the security of data, protection of which could be adequately dealt with through technology, but more to do with the significant amount of personal data which would lead to "function creep" with the inclination of the participating entities, government departments and/or private sector organizations, to access and use the data for purposes beyond the original ones of data collection, rationalizing such actions under the banner of public interest or business interest.

2. Here I wish to point out that in our annual community opinion surveys, the importance and significance of privacy as a social issue has been consistently rated highly, in fact the third highest just after unemployment and environmental pollution and higher than other important issues of food hygiene and hospital services. Please refer to the attached chart. Given its significant sociological impact, we strongly urge the Government to open other channels of communications, in addition to LegCo, to seek views from the community on the new I.D. Card before concluding its strategy.

3. We are heartened by the Government's plan to undertake privacy impact assessments at relevant stages of this project. We wish to emphasize that, apart from assessing the impact from technological and security perspectives, the societal impact should be adequately addressed, given the sentiments and expectations of our community with respect to privacy.

4. If in the overall Government consideration the new I.D. Card will serve multiple applications, our citizens should have a discretionary choice on the applications on offer. In other words, the citizens would regard the card, apart from its use for identification, as an optional mean to acquire or access to services at their discretion. It should be a genuine and non-discriminatory choice.

I appreciate your pertinent attention and consideration of these salient observations here as well as those in my earlier letter to you dated 15 March 2000 on the same subject. I reiterate our desire to assist in this significant Government initiative to further the betterment of our community.

Yours sincerely

Stephen Lau
Privacy Commissioner for Personal Data

Encl.

cc Mr Ng Hon Wah, HAB

APPENDIX 4

MEETINGS WITH STAKEHOLDERS

Date	Meeting with:
Mon 21 August	T P Wong, Deputy Director Helen Chan, APIO Special Assignment Section, Immigration Department
	Tony Lam, Deputy Privacy Commissioner for Personal Data.
Tues 22 August	Registration of Persons Sub-Division, Immigration Department KW Leung, APIO KW Chow, CIO Elaine Lo, CIO WS Ho, CIO and others
	Information Technology and Broadcasting Bureau (ITBB) Joyce Tam, PAS Alan Au, AS
Wed 23 August	Home Affairs Bureau Ng Hon Wah, PAS
	Information Technology Services Department (ITSD) Alex Ma, Assistant Director
	HK Police Sen Supt M R Demaid-Groves and others
Thurs 24 August	YM Li, PIO Information Systems (Production) Division, Immigration Department Ms Dorothy Chan, SSM and others
	Mr Clement Li, Deputy Chief Electoral Officer
Various times	Special Assignment Section, ImmD
Tues 12 September	HKSAR ID Card Project – Steering Committee – Presentation and Discussion
Thurs 14 September	T P Wong, Deputy Director Helen Chan, APIO Special Assignment Section, Immigration Department

APPENDIX 5

INTERNATIONAL EXPERIENCE

Overview of National Identity Card Schemes

Around 100 countries have official, compulsory, national identification schemes based on identity cards. They vary in design, purpose and the amount and type of information they contain. Examples of countries that have a national identity card are: Germany, Singapore, Portugal, Thailand, Korea, Chile, France, Belgium, Spain and Greece.

Countries that do not have national schemes often use identity cards or numbers to identify segments of the population for specific purposes, such as to prove eligibility for health or welfare services. Examples of countries that do not have a national identity card are: Japan, Canada, New Zealand, Ireland, The Netherlands, Australia, Denmark, the United Kingdom and the United States of America.

About 40 countries are actively planning to introduce national identity cards, or review existing schemes, as shown in the following table.

Countries Taking Steps to Implement National Identity Card Programs (September 1999)[1]

Argentina	Ethiopia	Namibia
Barbados	Estonia	Nigeria
Bolivia	Finland	Pakistan
Cambodia	Guatemala	Philippines
Cameroon	Indonesia	Republic of Korea
Chile	Ivory Coast	South Africa
China	Jamaica	Spain
Colombia	Madagascar	Syria
Costa Rica	Malaysia	Sudan
Dominican Republic	Mauritius	Thailand
Ecuador	Mexico	Uruguay
El Salvador	Mozambique	Venezuela
		Yemen

Paper based documents are being replaced by plastic cards containing bar codes, magnetic strips or computer chips. At the same time, governments are

[1] 'The National ID Movement', *ID World*, September/October 1999

reviewing the purposes for which the cards are used, and the information associated with them, in light of changing priorities and new technology.

In some cases, the way forward is not clear, due to changes in leadership, technological developments, financial shortfalls or community opposition. For example, Cambodia's plans to introduce a laminated card (with photo, personal data and fingerprints on a 2-dimensional bar code) to reduce fraud and strengthen border controls have been hampered by political instability. South Africa is also falling behind with its planned national identity smart card containing fingerprint data, to be used for pensions and other government benefits. A member of the consortium supplying and servicing the system has indicated that the delay has been caused largely by indecision about how extensive the scheme should be.[2] A proposal for a national identification system for the Philippines lapsed because the cost was under-estimated by eight billion pesos over seven years.[3] It was also found to be unconstitutional.[4]

The experiences of a sample of countries are summarised below.

Australia

National identity scheme

- In 1986, the Australian Government proposed to establish a national identity card called the Australia Card.
- It intended that the Australia Card would form the basis of the administration of major government agencies, link the finance and government sector, and perform the standard identification functions necessary in the commercial and Social Security sectors.
- The scheme's objectives changed many times during the two-and-a-half year campaign. It was primarily focused on reducing tax evasion, welfare fraud and illegal immigration.[5]
- The scheme was to comprise a register whereby participating agencies could share specified data about individuals. The entire population was to be recorded on the register, and every person was to have an obligation to acquire a code, and a card carrying the code, and to present that card in a wide variety of circumstances. The register was to facilitate front-end verification among participant agencies, and the identifier was to facilitate computer matching.[6]
- It caused such hostility that the proposed card was abandoned in 1987.

[2] Jim Aucoin, Polaroid Identification and Transaction Systems, quoted in 'The National ID Movement', *ID World*, September/October 1999
[3] Privacy International, *Identity Cards FAQs,* 1996
[4] Privacy International, *Country Reports,* 1999
[5] Roger Clarke, 'The Resistible Rise of the National Personal Data System', 23 October 1991
[6] *ibid.*

- When it withdrew the Australia Card Bill, the Government stated that it would instead adopt the recommendations of a Joint Select Committee of Parliament to the effect that the identification provisions relating to income tax be tightened. In May 1988, the Government announced details of proposed enhancements to the Tax File Number (TFN) scheme which had been in use within the Australian Tax Office (ATO) since the 1930s.[7]
- In December 1988 the amended TFN proposals were passed into law, along with the Privacy Act 1988, which created a set of highly qualified Information Privacy Principles and applied them to most agencies in the Commonwealth public sector. Guidelines relating to the use of TFN were established under the Privacy Act. The office of Privacy Commissioner was also established.
- The uses of the TFN have been extended over the years to permit a number of other limited uses by the Government, including cross-matching of data between the Australian Tax Office and assistance agencies using the tax file number in part of the process.
- Successive governments have distanced themselves from any proposals for a national identity card scheme. However, there are several programs to develop and extend national identification numbering systems. These range from national drivers licensing and vehicle registration schemes to plans for a cradle-to-grave national health identification number.
- A consortium of six State, Territory and City Governments has agreed on a national multiple application smartcard operating platform. The members are now working separately and together in introducing multiple smartcard applications. At this stage, none of the applications are national.

Privacy safeguards

- The *Privacy Act 1988* applies Information Privacy Principles to federal and ACT government departments and agencies. Special rules apply to the use of tax file number information and to credit information held and used by credit reporting agencies and credit providers.
- Privacy provisions exist in a number of other Commonwealth laws relating to information about health insurance claims, data matching, information about old criminal convictions and personal information disclosed by telecommunications companies.
- Legislation is presently before federal Parliament which, if passed, will extend the coverage of the *Privacy Act 1988* to most private sector organisations.

Public reaction

- The public debate about the Australia Card lasted from April 1985 until September 1987.

[7] *ibid.*

- Initially, there was little public resistance to the proposal, but opposition grew as the details became clearer. The card became the focus of a campaign of virulent opposition involving mass public protests and a party revolt. By mid-1987 there was intense public opposition to the scheme which ultimately led the Government to abandon the scheme.
- The opposition was based on concerns not only about privacy and but also cost. The official estimated cost of $820 million over seven years failed to take into account training and other administrative overheads for both government and business. The cost to the private sector alone was estimated to be over $100 million over ten years.[8]
- The public campaign against the Australia Card was spearheaded by the Australian Privacy Foundation, a group launched in August 1987, and comprising well-known Australians from all walks of life and all political persuasions.
- There remains a marked distrust in the community about proposals for national identification numbers. A proposal for a national health identifier has been discussed for many years by federal and State government agencies but has repeatedly stalled because of unresolved privacy issues. The introduction of a new national numbering scheme for businesses (the Australian Business Number) earlier this year was characterised by controversy about privacy and security implications.

Canada

National / Provincial identity scheme

- Canada presently does not have a national ID scheme. However there is continuing concern about the use of the Social Insurance Number (SIN) by the private sector and identity theft, as well as about the expansion of its uses, beyond its original purposes, by both the private and government sectors. A Parliamentary committee recommended in May 1999 that options be developed either to improve the SIN or replace it with a new card system. It recommended specific attention be given to privacy and data-matching issues as part of the process. [9]
- British Columbia gave consideration to provincial multi-function ID cards in 1994-95 but does not appear to have proceeded.

[8] Privacy International, *Identity Cards FAQs,* 1996

[9] "Beyond The Numbers: The Future Of The Social Insurance Number System In Canada", Report of the Standing Committee on Human Resources Development and the Status of Persons with Disabilities, May 1999, cited in Privacy International, *Country Reports*, 1999.

- Québec considered creating a mandatory ID card but dropped the idea in 1998. In April 1999, it hired DMR Consulting Group to examine the possibility of creating a central database of all government records on residents.[10]
- The Ontario Government announced in October 1999 that an Ontario Smart Card is to be introduced.
- The UN Human Rights Commission was critical of the increasing use of fingerprinting in Canada and recommended in April 1999 "that Canada take steps to ensure the elimination of increasingly intrusive measures which affected the right of privacy of people relying on social assistance, including identification techniques such as fingerprinting and retinal scanning."[11]
- In Toronto, a system to fingerprint all welfare recipients was dropped in March 1999 after Citibank, the contractor, was unable to create a working system.[12]

Privacy safeguards

- The Privacy Act of 1983 governs the privacy of personal information handled in the federal public sector.
- Privacy laws also exist at the provincial level, Québec being the only province with a privacy law governing both the public and private sectors.[13]
- The Personal Information Protection and Electronic Documents Act, a national law governing the handling of personal information in the private sector, comes into force on 1 January 2001.

Public reaction

- The Parliamentary Committee which looked at the future of the SIN expressed its significant concern with the threats to privacy associated with the current system.
- The Canadian Privacy Commissioner continually expresses concerns about the expanding uses of the SIN and the need for regulatory control of its use.[14]
- Public reaction to the Ontario smart card proposal was spearheaded by the Information and Privacy Commissioner, who put the view that any government smart card application must be respectful of the privacy of Ontarians and must not become a compulsory identity card designed as an instrument of surveillance. The Commissioner maintained that any smart card technology must be implemented in an open and transparent manner, with proper legislative controls and methods to ensure public accountability.

[10] Privacy International, *Country Reports*, 1999
[11] *ibid*.
[12] *ibid*.
[13] A number of the Canadian provinces (Ontario and British Columbia) are considering private sector privacy legislation. See Privacy Commissioner of Canada, *Annual Report: 1999-2000*.
[14] Privacy Commissioner of Canada, *ibid*.

- The Government has stated its commitment to protect privacy and to consult closely with the Commissioner in developing the proposal.[15]

China (other than the SARs)

National identity scheme

- Since April 1984, all mainland Chinese citizens over the age of 16 have been required to carry identification cards issued by the Ministry of Public Security, except active-duty members of the PLA and the People's Armed Police Force and inmates serving sentences.
- Identification cards include a photo plus name, sex, nationality, date of birth, address and term of validity, of which there are three. Between the ages of 16 and 25, it is 10 years, between the ages of 25 and 45, it is 20 years and for those aged 45 and over it is permanent.
- In carrying out their duties public security organs have the right to ask citizens to show their ID cards.
- In handling political, economic and social affairs, which involve rights and interests, government offices, people's organizations and enterprises may also ask citizens to show their ID cards. [16]
- Failure to register for an identification card, forging or otherwise altering a residence registration, or assuming another person's registration are all prohibited by law and punishable by fine.
- Failure to notify local authorities concerning visiting guests is also punishable by fine.[17]
- In 1997, the State Bureau of Technical Supervision began working on a new number system that will be used for Social Security and ID cards.[18]
- 1.1 billion paper identity cards have been issued – according to some reports [19] (another says that, as of early 1987, only 70 million people had been issued identity cards, well below the national goal and that even those with resident identity cards preferred to use other forms of identification[20]).

---

[15] Information and Privacy Commissioner, Ontario, *1999 Annual Report*

[16] Xinhua news agency, Beijing, in English, 7 May 1984, via BBC Summary of World Broadcasts; Regulations of the People's Republic of China Concerning Resident Identity Cards (Adopted at the 12th Meeting of the Standing Committee of the Sixth National People's Congress, promulgated for implementation by Order No. 29 of the President of the People's Republic of China on September 6, 1985, and effective as of September 6, 1985) CHINALAW No. 304.

[17] Chinalaw Computer-Assisted Legal Research Center Peking University – Regulations of the People's Republic of China on Administrative Penalties for Public Security (Adopted at the 17th Meeting of the Standing Committee of the Sixth National People's Congress, promulgated by Order No. 43 of the President of the People's Republic of China on September 5, 1986, and effective as of January 1, 1987) CHINALAW No. 368

[18] 'China: Numbering system aids social security,' *China Daily*, November 27, 1997.

[19] The National ID Movement', *ID World*, September/October 1999

[20] 'China Opens Doors to Smart Cards' Sep. 30, 1998 *Retail Delivery News*, vol. 3, no. 19 via comtex

- At the June 1999 Smart Cards China '99/CardTech/SecurTech China '99 conference in Beijing, Professor Qui Xue Xin of the Ministry of Public Security's police research institute predicted that China will issue 20 million to 40 million contactless smart cards carrying a digitized image of the cardholder's fingerprint in 2001, and that eventually more than 800 million Chinese adults will have them. At that time, however, the project was yet to be approved by the national legislature.[21]

Privacy safeguards

- Article 37 of the Chinese Constitution provides that the 'freedom of the person of citizens of the People's Republic of China is inviolable,' and Article 40 states: 'Freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law. No organization or individual may, on any ground, infringe on citizens' freedom of privacy of correspondence, except in cases where to meet the needs of state security or of criminal investigation, public security or prosecutorial organs are permitted to censor correspondence in accordance with procedures prescribed by law.' [22]
- Outside the Hong Kong SAR, there is no general data protection law in China and few laws that limit government interference with privacy.

Public reaction

- Not known
- Anecdotal evidence indicates some opposition:

> We have to use it in almost every situation such as renting a hotel room, getting legal service from lawyers, contacting government agencies, buying a plane ticket and train ticket, applying for a job, or getting a permit to live with your parents, otherwise your residence is illegal. In a lot of cases, we are showing too much irrelevant information to an agency or person who could not know that. The card is subject to police cancellation, and thus, without it, one can hardly do anything, including traveling for personal or business purposes, or getting legal help or obtaining a job. The government has been using this scheme too often as a measure against persons who run into trouble with it socially or politically. The identity card is showing your daily or every short-term

[21] The National ID Movement', *ID World*, September/October 1999

[22] PRC Constitution from ChinaLaw Web - Constitution of the People's Republic of China – 1993 (Adopted at the Fifth Session of the Fifth National People's Congress and Promulgated for Implementation by the Proclamation of the National People's Congress on December 4, 1982, as amended at the First Session of the Seventh National People's Congress on April 12, 1988, and again at the First Session of the Seventh National People's Congress on March 29,1993.)

movement, and can be used to regularize and monitor a person's behaviour and activity.[23]

Estonia

National identity scheme

- The passports currently carried by Estonian citizens start to expire in 2002. It has therefore been decided that thereafter two types of personal identification documents shall be issued: an ID-card that is going to serve as a multifunctional national passport and allows citizens to cross the European borders, and an international passport that will only be used for travelling outside the EU.
- On May 11, 1998, the Estonian Minister of Interior Affairs issued a directive, establishing the 'Commission for developing and publishing the ID-card and its technical specification'. The Commission, consisting mostly of government officials, developed and represented the governmental policy regarding the ID-card.
- The card is to be multifunctional - besides being a nationally accepted personal identification token, it will also serve other purposes, both in the public (social security, health insurance etc) and private sectors (banks, service companies etc).
- It may eventually include biometrics.
- Cards will require PINs and be issued to persons 16 years and older.[24]
- Expected to cost between $1million and $2million for up to 800,000 cards.[25]

Privacy safeguards

- Article 42 of the 1992 Estonian Constitution states, 'No state or local government authority or their officials may collect or store information on the persuasions of any Estonian citizen against his or her free will.' Article 44 (3) states, 'Estonian citizens shall have the right to become acquainted with information about themselves held by state and local government authorities and in state and local government archives, in accordance with procedures determined by law. This right may be restricted by law in order to protect the rights and liberties of other persons, and the secrecy of children's ancestry, as well as to prevent a crime, or in the interests of apprehending a criminal or to clarify the truth for a court case.'
- Estonia's Personal Data Protection Act of 1996 protects the fundamental rights and freedoms of persons with respect to the processing of personal

[23] Simon Davies 'A Case of Mistaken Identity: An International Study of Identity Cards' (prepared for the Information and Privacy Commissioner/Ontario), April 1995
[24] Estonian Government website
[25] The National ID Movement', *ID World*, September/October 1999

data and in accordance with the right of individuals to obtain freely any information which is disseminated for public use. The Act divides personal data into two groups – non-sensitive and sensitive personal data. Sensitive personal data are data which reveal political opinions, religious or philosophical beliefs, ethnic or racial origin, health, sexual life, criminal convictions, legal punishments and involvement in criminal proceedings. Processing of non-sensitive personal data is permitted without the consent of the respective individual if it occurs under the terms that are set out in the Personal Data Protection Act. Processed personal data are protected by organizational and technical measures that must be documented. Chief processors must register the processing of sensitive personal data with the data protection supervision authority.

- The Databases Act of 1997 is a procedural law for the establishment of national databases. The law sets out the general principles for the maintenance of databases, prescribes requirements and protection measures for data processing, and unifies the terminology to be used in the maintenance of databases.
- The Data Protection Department of the Ministry of Internal Affairs is the supervisory authority for the Personal Data Protection Act and the Databases Act. [26]

Public reaction

- Not known.
- According to Estonian press reports in November 1996, databases of the financial and police records of thousands of Estonians have been easily available on the black market. The records were available on CD-ROM and sold for $4,000 each, and included details of individual's bank loans and police files.[27]

Finland

National identity scheme

- In December 1999, the Finnish Ministry of Interior, through the Population Register Centre, issued the world's first electronic national ID card (called FINEID). The first batch of cards were being issued to public servants and then to the entire nation.[28]
- Applying for the card is voluntary.

[26] Privacy International, *Country Reports,* 1999
[27] The Baltics Worldwide, Spring 1997.
[28] Hong Kong Immigration Department, 'Feasibility Study on the HKSAR ID Card System: Market Research Report', 11 April 2000.

- Finnish citizens over the age of 18 years (under 18 with parental consent) can order their ID smart card from their local police authority. It is valid for 3 years. The card can be used in smart card readers included in PCs in the home and the workplace. In future, the smart cards have the capability to be used in conjunction with WAP (Wireless Application Protocol) mobile phones and digital interactive television.
- The card carries the card holder's visual demographic data and other security features, and the electronic identity of the card holder.
- Cards have a microprocessor chip with 16 kilobytes of memory, and feature citizens' photos. The Finnish Population Register Centre is responsible for manufacturing and distributing cards, creating keys and issuing and storing digital certificates.
- The multi-application contact smart cards includes:
    - National ID
    - Bank card
    - Credit card
    - Functions for riding public transport.

Privacy safeguards

- Through public key technology, electronic certificates are issued and stored on the card. Separate RSA key pairs are used to generate digital signatures and certification/encryption services and non-repudiate e-transactions and e-commerce.[29]
- The Personal Data Protection Act 1999 came into effect on June 1, 1999. The law replaced the 1987 Personal Data File Act to make Finnish law consistent with the EU Data Protection Directive.
- The Data Protection Ombudsman (DPO) enforces the Act and receives complaints. The office conducted 450 complaints and 10 investigations in 1998. It also receives 5,000-8,000 requests for advice each year. A Data Protection Board resolves disputes and hears appeals of decisions rendered by the DPO. It also determines if personal information can be exported.[30]
- The Finnish Government has enacted special ordinances that apply to particular personal data systems. These include those operated by the police such as criminal information systems, the national health service, passport systems, population registers, farm registers, and the agency responsible for motor vehicle registration.[31]
- The Population Register Centre, part of the Finnish Government's Ministry of the Interior, serves as the Certificate Authority for the electronic exchange of official information. Its task is to provide basic electronic identity to the citizens. In administration, the Centre is responsible for providing the government certificate services and creating and maintaining the infrastructure required

[29] HKSAR Immigration Department, 'Feasibility Study on the HKSAR ID Card System', *ibid*.
[30] Privacy International, *Country Reports*, 1999.
[31] *Ibid*.

for the system. The Centre is also involved in many related national and international projects.[32]

Public reaction

- Not known.

France

National identity scheme

- France has a voluntary national ID scheme.
- A (compulsory) paper-based national identification system was in force until the late 1970s.
- In 1979, the Ministry of the Interior announced plans for an automated card encased in plastic, to be used for anti-terrorism and law enforcement purposes, to be issued to all 50 million residents of France and to be phased in over 10 years.
- With the 1981 election to government of the Socialists, the ID card proposals went into demise.
- In 1986 the newly-elected conservative government reintroduced plans for an upgraded national ID card. It was proposed to have a machine readable card with a fingerprint on the application form.

Privacy safeguards

- CNIL approved the proposal but made certain rulings which meant the card was not compulsory, because individuals would retain the right to identify themselves by any means.
- The ID card machinery cannot be linked to registers, nor can the information be given to third parties.
- The Data Protection Act of 1978 covers personal information held by government agencies and private entities. It is being amended to make it consistent with the EU Directive.[33]

Public reaction

- In 1980, after the Government announced plans to upgrade the paper based national identity document to a higher integrity plastic card, the Union of

[32] Population Register Centre's website:http://www.vaestorekisterikeskus.fi/
[33] Privacy International, *Country Reports,* 1999

Magistrates said the card had the potential to limit the right of free movement.[34]
- Political and public opposition grew as details of the plan became known. There were concerns over the possible impact of such cards.
- The Commission Nationale de L'informatique et des Libertés (CNIL) managed to suppress the machine readable function of the proposed cards though optical scanning made magnetic stripes somewhat redundant.
- CNIL also ruled that no number relating to an individual could be used, but that each card would carry a number.
- Publications such as Le Figaro expressed concern that the cards and related information could be linked with other police and administrative systems.
- When the card was introduced on an experimental basis in 1988, media and civil liberties groups expressed strong adverse reaction.[35]

Greece

National identity scheme

- Greece has a compulsory identity card system (named 'Single Register Code Number').
- The number is the official national ID number for the population register, ID card, voting register, passport number, tax number, driver's license number, and other registers.[36]
- All citizens from the age of 14 years must carry the card.

Privacy safeguards

- The law of 1599/1986 (Law no 1599/1986 on the relationship of a new type of identification card and other provisions) regulates the use of the Single Register Code Number.
- The Law on the Protection of Individuals with regard to the Processing of Personal Data was approved in 1997. Greece was the last member of the European Union to adopt a data protection law and its law was written to apply the EU Directive into Greek law.[37]

[34] Privacy International 'Identity Cards: Frequently Asked Questions', August 24, 1996
[35] Simon Davies, 'A Case of Mistaken Identity: An International Study of Identity Cards' (prepared for the Information and Privacy Commissioner/Ontario), April 1995,
[36] Privacy International, *Country Reports*, 1999
[37] *ibid*.

Public reaction

- The European Parliament passed a resolution in 1993 calling on the Greek Government not to place religion on its national ID cards. Greece was the only EU nation that required citizens to declare their religious beliefs.
- In July 2000, the Greek Government issued a decree formally abolishing religion from the ID card. It also abolished fingerprints, occupation and spouse's name, while adding a blood type option as well as Latin characters to allow easy travel in the 15-nation European Union.
- Greek Orthodox leaders fear the removal of the religious label could be a first step toward a separation of church and state. The Greek Orthodox faith is the official state religion. Church leaders, urged on by firebrand Archbishop Christodoulos, warned they will take whatever action necessary to stop the move. Christodoulos has demanded a national referendum.
- Although church attendance is low in Greece, the Orthodox faith figures prominently as a common point of national and ethnic identity. Many church leaders are deeply suspicious of the Government's drive to make Greece a modern European country.
- Greece's church has said it will try to collect nearly 5 million signatures in this country of 10.5 million people to force a national referendum on the decree. It has asked all adult Greeks to declare their desire for a referendum, even though the Government has said it will not hold one. Some of Christodoulos' senior clerics have expressed hope that the Government will collapse because of the campaign and a series of mass rallies.
- The Government has ruled out the possibility of a referendum and referred to Christodoulos as a private individual who has the right to freely express his views.
- Premier Costas Simitis' Socialist Government has said the religion entry on the ID cards ran counter to Greece's modernization efforts. It also says the church's signature campaign could endanger the unity of the Greek people.[38]

Korea

National identity scheme

- In 1997, the Government announced the creation of an ‘Electronic National Identification Card Project’.
- The project was based on a multi-purpose smart card system and according to a local human rights group would ‘include universal ID card, driver's license, medical insurance card, national pension card, proof of residence, and a scanned fingerprint, among other things’. It would consolidate the functions of ID card, driver's license, and medical insurance card.

[38] Patrick Quinn, ‘Greece Abolishes Religion from IDs’, Associated Press, 17 July 2000

- It was a US$413 million project managed by the Ministry of Domestic Affairs.[39]
- The Government was scheduled to issue cards to all citizens by 1999. On November 17 1997, a law on the ID card project passed the National Assembly.
- The City of Seoul started to issue the Card to 1,000 citizens as a 'test' in March 1997.
- In December 1997, Kim Dae Jung won the Presidential election. He had publicly opposed the ID card project in his campaign and it appears to have stopped. However, activists believe that government agencies are continuing to quietly develop the proposals.[40]

Privacy safeguards

- The Act on the Protection of Personal Information Managed by Public Agencies of 1994 sets rules for the management of computer-based personal information and is enforced by the Minister of Government Administration.
- The effect of this law on the proposal was uncertain, as was the legal basis for the card (and the `test'). [41]

Public reaction

- Strong opposition from the community, including activists who brought international attention to the issue.

Malaysia

National identity scheme

- A multi-purpose national identity smart card scheme is presently being implemented by the Malaysian Government – in association with a consortium of 5 companies. There will two multipurpose cards, although only one was initially planned. They will be merged in the future.
- The card will be issued to all Malaysians from the age of 12 years.
- The first card is to be launched in two batches. The first batch, on 1 November 2000, will be the government multipurpose card (GMPC) containing personal, immigration and driving licence details of the cardholder. Between 10,000 to 50,000 will be rolled out.

[39] Korean telecommunications company DACOM, which won the bidding for the project http://bora.dacom.co.kr/bora/ dacom/news-clips.html

[40] Privacy International, *Country Reports*, 1999

[41] Privacy Law and Policy Reporter, 1996 vol 3 p 60

- The second batch of the GMPC will be rolled out on 1 April, 2001. Together with the above details, it will also have health details and option e-cash. About 2 million cards will be rolled out initially.
- The second multipurpose card, which facilitates payment and banking facilities, will be rolled out in January 2001 up to December 2004. Automatic teller machines will eventually be phased out. [42]
- The contact smart card will be supplied by IRIS technology with 32K memory chip for storing fingerprint and black and white photo image of the card holder.
- While initial applications require only contact card technology, it is envisaged that contactless card technology will be added to the multi-purpose card platform later. The multi-purpose card is not an isolated project by itself. It is designed to act as the medium for users to interface with other 'Multimedia Super Corridor' initiatives.
- The multi-purpose smart card will act mainly as
    - a national ID card
    - a driving license
    - medical record
- The card will also include immigration functions to expedite passenger clearance, especially for those who travel frequently to Singapore and Thailand.
- The objectives of each of the four initial government applications and optional E-cash scheme are detailed below.

    National ID
    - To improve the security of the current national ID card.
    - To serve as an access key that uses the ID number to provide secure access to other applications or systems.

    Driving Licence
    - To replace paper-based, laminated driving licence card with an application providing enhanced security of information;
    - To enhance traffic law enforcement by providing officers with immediate, dynamic driving records; and
    - To increase accuracy of summons information in JPJ and police databases, blacklists and fine payment systems.

    Immigration
    - To supplement the International passport to expedite immigration clearance for Malaysian passport holders;
    - To enhance immigration control at border point;
    - To reduce time required to issue and renew international passport; and
    - To improve accuracy of entry and exit data captured in Jabatan Imigresen Malaysia (JIM) databases.

[42] 'The Seven Different Flagships' *The Star*, 4 September 2000

Medical
- To provide a portable record of basic medical data;
- To serve as an access key to a patient's medical records in a MOH's proposed database;
- To improve treatment in emergency and general care situations; and
- To facilitate communication between public and private health care providers through the means of a homogenous health care network and medical record system.

E-cash (optional):
- To improve speed and convenience of low value payments;
- To reduce cash as a means of payment;
- To provide better security against fraud and counterfeiting; and
- To provide an E-cash application for both government and payment MPCs.

- For the Malaysian public the GMPC is presented as a means to better and more effective services. The card in conjunction with other MSC initiatives would enable them to access public services and facilities electronically 'at a touch of a button'. Some of the potential access key applications are the EPF transactions, voter registration, payment transactions, ticketless travel, student card and car park access, to name a few. Transactions could be done in a shorter time with no or minimal paperwork involved.

- The proposal is very similar to one that South Africa has said it intends to pursue.

Privacy Safeguards

The Malaysian Government website does not mention privacy but does say that -

- Legislation needs to be changed or amended to recognise the individual rights and dependence on the card. For example it is no longer possible to impound a person's driving license since that would deprive him of his ID and access to his cash in the E-Cash application.

- Malaysians were told in 1998 that if they do not carry their cards, they risked being detained by immigration police.[43] In January 1999, it was announced that Muslim couples married in the Malaysian capital will be issued cards with computer chips so Islamic police can instantly verify their vows and the police will be equipped with portable card readers. In December 1998, the Government began requiring that cybercafes obtain name, address, and

[43] 'Malaysians told: Carry ICs or risk detention', *New Straits Times*, May 14, 1998

identity card information from patrons but lifted the requirement in March 1999.[44]

- The Constitution of Malaysia does not specifically recognize the right to privacy.
- The Ministry of Energy, Communications and Multimedia is drafting a Personal Data Protection Act that will create legal protections for personal data as part of the 'National Electronic Commerce Master Plan.' Secretary-general Datuk Nuraizah Abdul Hamid said the purpose of the Bill was to ensure secrecy and integrity in the collection, processing and utilization of data transmitted through the electronic network.

Public reaction

- Not known

New Zealand

National identity scheme

- There is no national ID scheme in New Zealand.
- In 1991 the Government drew up a health care and social welfare reform plan involving the development of a data matching program and a national identity card.
- The ID card proposal did not subsequently proceed. The controversy surrounding the proposed card resulted in the abandonment of the card and the adoption of a low integrity entitlement card for the purpose of health benefits.[45]
- In March 1998 the Privacy Commissioner commented on legislation then before Parliament (The Land Transport Bill) which proposed to replace lifetime driver's licences with a 10-year renewable credit-card sized licence, bearing a digitised photograph. The Commissioner saw the proposal as creating conditions for a de facto national ID card.
- The proposal would oblige drivers to carry the licence at all times while driving.
- The Commissioner also criticised the driving licensing privacy impact assessment published by the Land Transport Safety Authority on grounds that its value is severely diminished 'when all the key decisions seem to have been taken or presented as foregone conclusions and most people will be unaware of its existence.'[46]

[44] Cabinet: Cybercafes not subjected to restrictions', *New Straits Times*, March 18, 1999
[45] Simon Davies, 'A Case of Mistaken Identity: An International Study of Identity Cards' ((prepared for the Information and Privacy Commissioner/Ontario), April 1995.
[46] *Private Word*, Issue no 23, March 1998

- The High Court, in a decision on application for judicial review of the law (which was passed in 1998) also criticized the inadequacy of the privacy impact assessment undertaken by the Ministry of Transport.

Privacy safeguards

- New Zealand Privacy Act applies Information Privacy Principles to the private and public sectors. The Information Privacy Principles are generally based on the 1980 OECD guidelines and the information privacy principles in Australia's Privacy Act 1988.
- The legislation includes a principle that deals with the assignment and use of unique identifiers.

Public reaction

- People were particularly concerned about the right of the Government to hold 'power' over the citizen.
- A campaign of opposition was formed in August 1991 under the leadership of the Auckland Council for Civil Liberties.
- Significant controversy surrounding the proposed card resulted in the abandonment of the card and the adoption of a low integrity entitlement card for the purpose of health benefits.

Philippines

National identity scheme

- The Adoption of a National Computerized Identification Reference System was introduced by former President Ramos in 1996 via Administrative Order No 308.
- The Supreme Court ruled in July 1998 that the Administrative Order was unconstitutional.
- The Court said that the order, 'will put our people's right to privacy in clear and present danger . . . No one will refuse to get this ID for no one can avoid dealing with government. It is thus clear as daylight that without the ID, a citizen will have difficulty exercising his rights and enjoying his privileges.'
- The main reason that the proposal lapsed is reportedly the fact that the Government under-estimated the cost by eight billion pesos over seven years.[47]
- President Joseph Estrada reiterated his support for the use of a national identification system in August 1998 stating that only criminals are against a

[47] Privacy International, *Identity Cards FAQs,* 1996

national ID.

- Justice Secretary Serafin Cuevas authorized the National Statistics Office to proceed to use the population reference number for the Civil Registry System-Information Technology Project on August 14, claiming that it is not covered by the decision.
- It is reported that the Philippines is developing a biometric based ID scheme.

Privacy safeguards

- The 1987 Constitution protects the right of privacy.
- There is no general data protection law but there is a recognized right of privacy in civil law.

Public reaction

- Not known.

Singapore

National identity scheme

- Singapore identity cards were introduced in 1948 by the colonial government under the 1948 National Registration Ordinance.
- A new identity card scheme was introduced by an independent Singapore on 6 May 1966. It comprises a Pink Identity Card for Singapore citizens, and a Blue Identity Card for permanent residents. It also led to the introduction of unique ID numbers.
- In 1991, credit sized identity cards were introduced, with new security features (bar-coded card number; electronically captured thumbprint and photo; changeable laser image of Singapore's lion head logo; holder's unique ID number).
- 1,233,705 people have registered
- Officially, the purpose of the card is to 'identify those born in Singapore and weed out illegal immigrants and other undesirables'.
- The Scheme is administered under the 1966 National Registration Act[48]

Immigration control

[48] Singapore Government Website http://www.gov.sg

- Singapore citizens and permanent residents can obtain travel cards (Access Cards) valid for two years. It takes only 15 seconds for the scanners at Changi Airport and the bus passenger halls of the Woodlands and Tuas Checkpoints to match a traveller's thumbprint to the one stored on the card.
- Travellers with the cards have immigration clearance through automated lanes at the checkpoints.
- At the automated lanes, the card holder inserts the Access Card into a reader and places his/her right thumb on the fingerprint scanner for verification.
- No application form is required to get a card, but travel documents and a passport photo must be given.
- The card is valid for 2 years.
- It is not a substitute for a valid travel document[49]

Privacy safeguards

- The Singapore Constitution does not contain any explicit right to privacy.
- There is no general data protection or privacy law in Singapore.[50]

Public reaction

- Not known

Taiwan

National identity scheme

- There is presently no national ID scheme in Taiwan. One was proposed in 1997 but did not subsequently proceed.

- Features of the 1997 proposal[51]:
  - Was called the 'National Integrated Circuit (IC) Card.'
  - It was proposed that a private company (Rebar Corporation) set up and pay for the system, issue cards and operate the system, as well as receive any profits from its creation. The entire system was estimated to cost NTD 10 billion (USD 357 million).
  - Over 100 uses were proposed for the smartcard, including ID, health insurance, driver's license, taxation and possibly small-value payments.

[49] Singapore Government Website http://www.gov.sg
[50] Privacy International, *Country Reports*, 1999
[51] Privacy International, *Country Reports*, 1999

    - There were hearings to evaluate privacy concerns after protests about the plan arose. Rebar withdrew from the project in November 1998 over costs and amid public protests.
- The Government is now considering creating its own paper-based card, and may later transfer it to a private company for operation. It is also now considering a smartcard-based system just for health information.
- Also, Taiwan officials are reportedly looking closely at introducing an immigration-control system along the lines of the Singapore Immigration Automated Clearance System (IACS).

Privacy safeguards

- Article 12 of the 1994 Taiwanese Constitution states: 'The people shall have freedom of privacy of correspondence.'
- The Computer-Processed Personal Data Protection Law was enacted in August 1995. The Act governs the collection and use of personally identifiable information by government agencies and many areas of the private sector, but only in respect of computer processing systems with personal data.[52] The Act also establishes separate principles for eight categories of private institutions: credit information organizations, hospitals, schools, telecommunication businesses, financial businesses, securities businesses, insurance businesses, mass media, and 'other enterprises, organizations, or individuals designated by the Ministry of Justice and the central government authorities in charge of concerned end enterprises.'
- There is no single privacy oversight body to enforce the Act. The Ministry of Justice enforces the Act for government agencies. For the private sector, the relevant government agency for that sector enforces compliance. The Criminal Investigation Bureau (CIB) arrested several people in November 1998 for selling lists of more than 15 million voters and personal data of up to 40 million individuals in violation of the Act[53].

Public reaction

- Not known.

[52] 'The Asian Status with respect to the observance of the OECD Guidelines and the EU Directive by Stephen Lau, Privacy Commissioner for Personal Data Hong Kong, 19th International Conference of Privacy Data Protection Commissioners, Brussels, Belgium, September 17 - 19, 1997'
[53] Privacy International, *Country Reports*, 1999

Thailand

National identity scheme

- Thailand has a national ID card system; identity cards having been issued to the Thai population by 1997.
- Every Thai adult has a machine readable ID card (magnetic strip) containing a digitized thumbprint and photograph, details of family and ancestry, education and occupation, nationality, religion, and information relating to taxation and police records.
- The card can be scanned by any police or government official to activate a nationwide network of computers throughout the Thai Government.
- A number of government departments are linked to the system, including the Revenue Department, the Ministry of Foreign Affairs, the Ministry of Defence and the Office of the Narcotics Control Board. By using a person's population number, which is registered in all agencies and banks, it is possible to secure information from police, social welfare, taxation, immigration, housing, employment, driving licence, census, electoral, passport, vehicle, insurance, education and health record databases.
- The Government also plans to link the system with other governments to allow holders to travel in Asian countries without the need for a passport, using only the new card. Bank customers who carry the new ID card can use it as an ATM card as well.[54]
- A separate (but presumably linked) initiative commenced in 1995, when Control Data Systems was awarded a $11.5 million contract by the Bangkok Metropolitan Administration (BMA) project to install the Computerized National Census and Services Project. The system includes names, addresses, national ID card numbers, and census information such as birth and death records and address changes. It will be used for checking individual tax returns and compiling census statistics. It was expected to be completed by the time of the elections in 2000[55]. It is not known what stage the project has achieved.

Privacy safeguards

[54] ' The Thai Ministry of Interior maintains the second-largest relational database in the world ... In conjunction with the Central Population Database project, the Ministry of Interior introduced a new identity card issuing project in early 1994 ... An image of the person's right thumbprint is scanned and stored in the national database at the time of card creation. The card contains printed biographical information and an identification photograph on the front side, and a magnetic strip containing biographical information and a reference to the person's thumbprint on the back side' (technology-provider LSC Inc.'s promotional material).

[55] Privacy International, *Country Reports*, 1999

- It is not known whether any specific privacy safeguards apply to the operation of the card.
- The National Information Technology Committee (NITC) approved plans in February 1998 for a series of information technology laws. Six sub-committees under the National Electronics and Computer Technology Centre are drafting laws on E-Commerce Law, EDI Law, Privacy Data Protection Law, Computer Crime Law, Electronics Digital Signature Law, Electronics Fund Transfer Law and Universal Access Law. The first three, the electronic commerce law, a digital signature law and the electronic fund transfer law are expected to be completed in 1999 and submitted to the Parliament. [56] The electronic commerce and electronic digital signature laws have been approved by Cabinet and as at June 2000 were under considered by Thailand's Government Legislation Committee. [57] The second group of laws is expected to be completed in 2000.

Public reaction

- A paper by Simon Davies reported that the introduction of the ID card apparently gave rise to little concern among Thai residents.[58]

United Kingdom

National identity scheme

- There is presently no national identity card system in the UK, although there have been a number of proposals for identity cards over the years.[59]
- Unsuccessful attempts to introduce a national identity card schemes included:
    - 1988 – Tony Favell's proposed Bill to introduce a British Identity Card
    - 1988/89 – Ralph Howell's National Identity Card Bill
    - 1989 – Jacques Arnold's proposed Bill to introduce a Unique Personal Identity Number

[56] Privacy International, *Country Reports*, 1999

[57] *The Nation*, 27 June 2000. Also see *The Nation*, 5 February 2000, which reported that the Association of Thai Computer Industry wants the agency overseeing the drafting of the electronic transaction law to focus its attention next on a related e-commerce law to protect consumer privacy in commercial transactions over the Internet.

[58] Simon Davies, 'A Case of Mistaken Identity: An International Study of Identity Cards' (prepared for the Information and Privacy Commissioner/Ontario), April 1995. In his paper Davies cites a *Bangkok Post* article dated 17 February 1991 entitled 'The fear of Big Brother', which may shed further light on public reaction to the ID card proposal. (Unable to obtain.)

[59] Simon Davies' paper 'A Case of Mistaken Identity: An International Study of Identity Cards' (prepared for the Information and Privacy Commissioner/Ontario), April 1995, provides historical background on the proposed ID card scheme in the UK in 1994/95. Also see 'Identity Cards – Putting you in the picture', An information pack from the Data Protection Registrar, (undated, probably mid-1995).

  - 1993 – David Amess's proposed Bill to introduce a voluntary Personal Security Card
  - 1994 – Harold Ellotson's National Identity Card Bill.[60]
  - 1995 – Home Secretary's Green Paper on Identity Cards.
    - (Followed the 1994 Tory Party conference when more than 40 motions calling for ID cards were received.[61])
    - Divisions of opinion about the introduction of ID cards existed both within the Government and Opposition.[62] Opposition to the idea of a compulsory card was either on libertarian grounds or on the basis that they would accelerate European integration.[63]
    - The ID card proposal was ultimately abandoned by the Labor Government in 1996.

- The most recent proposal was reported by the press in May 2000 when it was revealed that the UK Passport Agency's 5-year business plan included a proposal for a photocard passport involving a 'credit card' style travel document designed to ease travel in Europe. The plan reportedly suggested that by 2005 the Government may have built a national identity database and that passport pictures could be replaced by other means of identity, such as electronic fingerprinting and automated facial recognition. Development work will take place on the assumption that European leaders could agree its launch in the 'next couple of years'.[64]
- This report is consistent with an announcement made in 1999 by Home Secretary Jack Straw that the UK Government was considering a new voluntary national ID card for all Britons to replace passports. He said that government was also looking into using the card for 'combined tax and benefits smartcard, as well as a scheme already due to come into force for a photo-ID driving licence.'[65]

Privacy safeguards

- The UK does not have a written constitution. In 1998, the Parliament approved the Human Rights Act that will incorporate the European Convention of Human Rights into domestic law, a process which will establish an enforceable right of privacy. The Act will go into force in October 2000.
- The Parliament approved the Data Protection Act (1998) in July 1998. It updates the 1984 Data Protection Act in accordance with the requirements of the European Union's Data Protection Directive. The Act covers records held by government agencies and private entities. It provides for limitations on the

[60] UK Data Protection Registrar, *ibid*.
[61] Simon Davies, *ibid*.
[62] *ibid.*
[63] *ibid.*
[64] *The Times,* 6 May 2000
[65] *The Times of London,* 30 June 1999

use of personal information, access to records and requires that entities that maintain records register with the Data Protection Commissioner.
- The Office of the Data Protection Commissioner is an independent agency that enforces the Act. Under the previous act, a total of 225,000 organizations and businesses registered, although this figure is believed to fall well short of the total number of entities that qualify to register.
- There are also a number of other laws containing privacy components, most notably those governing medical records and consumer credit information.[66]

Public reaction

- When the Government's Green Paper on Identity Cards was released in 1995, the idea was supported by 74% of the population. However, two years later the proposal was abandoned, following division within the Government and strong opposition from the community. One Government MP described ID cards as 'the biggest extension of state power since the introduction of income tax.' The Social Security Minister opposed it on the grounds that it would not stop fraud. There was also a fear that citizens would effectively be required to carry the card at all times, even though it was supposed to be a voluntary scheme. Finally, in order to make the scheme pay for itself, each card holder was going to have to pay 10-15 pounds for a card.[67]
- The UK Data Protection Registrar's response to the Government's 1995 Green Paper on Identity Cards expressed significant concerns about the possible introduction of ID cards. Among the specific comments were:
    - Additional statutory safeguards would be needed
    - Opposed to the inclusion of personal information with a personal identification number.
    - The Registrar was not persuaded a national ID card would substantially assist in preventing and detecting crime.
    - The holding of biometric information, in particular finger scans, raises genuine concerns about the safeguards to prevent its further use.
    - A photographic driving licence (as an alternative) may develop into a de facto national ID card.
    - Clear identification of purpose needed; likewise, of relative responsibilities if a number of organisations involved.
    - DPR should be the relevant enforcement authority if an ID scheme set up.

- Results of the DPR's consultations on the subject were also included: A majority (54%) of people who responded to the DPR's consultation pack (over 1000 responses) were opposed to the introduction of any identity card. The reasons cited included:

[66] Privacy International, *Country Reports,* 1999
[67] Kirsty Milne, 'This week's skirmishes over ID cards reveal a government weak on tactics, strategy and policy direction' *New Statesman*, 23 August 1996

  - Concerns over civil liberties issues such as the loss of freedom and the right to remain anonymous.
  - Potential created for state monitoring of individuals, indicating either distrust of government, or potential for abuse by those in power.
  - Doubts that ID cards would have an effect on crime or act as a fraud deterrent; possibility for new types of crime to be created.
  - Concern over costs.
  - No sufficient justification for another identifier.
  - Purpose of the card should be made clear.
  - Concerns over who would have access to the information.
  - Likely drift from voluntary to compulsory use of the card.
  - Some said they would refuse to comply or carry the card.
- 46% of respondents were in favour of a card.
- DPR stated it was not possible to draw any firm conclusions about public attitudes based on responses to her, but nevertheless noted a clear disparity of view and clear lack of support for an ID card.

APPENDIX 6

BIBLIOGRAPHY AND RESOURCES

Resource	Source	On-line Location ?
Feasibility Study on the HKSAR Identity Card System (2 vols)	SITA for the HKSAR Immigration Dept, June 2000	
Market Research Study	SITA for the HKSAR Immigration Dept, April 2000	
Registration of Persons Ordinances and Regulations	HK Laws	http://www.justice.gov.hk/Home.htm
Privacy Law & Policy Reporter (PLPR) Various articles - see Smart cards Special Issue Vol 2 No 10 January 1996		Vols 1-4 on line at http://www.austlii.edu.au/au/other/plpr/
Electronic Privacy Information Centre Online privacy resource guide + links		http://www.epic.org/
Global Internet Liberty Campaign Annual world privacy survey + links		http://www.gilc.org/privacy/
Privacy International		http://www.privacyinternational.org/ pages on National ID cards http://www.privacy.org/pi/activities/idcard/
International Study of Identity Cards - Simon Davies	Ontario Privacy Commissioner, 1995	
Touching Big Brother – How biometric technology will fuse flesh and machine – Simon Davies	1994	http://www.privacy.org/pi/activities/idcard/
Identity Cards – Philip Thomas	Modern Law Review Vol 58 No 5, Sept 95	

Speech Notes – Provincial ID Cards - a Privacy Impact Assessment	British Columbia Privacy Commissioner 1995	
UK National ID Card Proposal 1988-89	Collection of papers, clippings and Hansard pages	
Identity Cards – Putting you in the Picture – Information Pack	UK Data Protection Registrar 1995	
Response to UK Government Green Paper on ID Cards	UK Data Protection Registrar 1996	
Population Registers: Some Administrative and Statistical Pros and Cons – Philip Redfern	Journal of the Royal Statistical Society, Vol 152, Pt 1, 1989.	
Decision of McGechan. J in McInnes and Minister for Transport (criticizes inadequacy of PIA for photo driver licence)	NZ High Court	
Chip based payment schemes: Stored Value Cards and Beyond	Roger Clarke, Xamax Consultancy, 1996	Some on-line at http://www.anu.edu.au/people/Roger.Clarke/EC/CBPSBk.html
Smart Cards as National Infrastructure	Governnent Technology & Telecommunications Committee (Aus) 1997	

Smart Cards and the future of your money	Centre for Electronic Commerce, Monash University, for the Australian Commission for the Future, 1996	
Chip-Based ID: Promise and Peril (1997)	Roger Clarke, Xamax Consultancy	http://www.anu.edu.au/people/Roger.Clarke/DV/IDCards97.html
Human Identification in Information Systems (1994)	Roger Clarke, Xamax Consultancy	http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html
Just Another Piece of Plastic for your Wallet: the 'Australia Card' Scheme (1987)	Roger Clarke, Xamax Consultancy	http://www.anu.edu.au/people/Roger.Clarke/DV/OzCard.html
The Resistable Rise of the National Personal Data System (1991)	Roger Clarke, Xamax Consultancy	http://www.anu.edu.au/people/Roger.Clarke/DV/SLJ.html
Smart Cards - Implications for Privacy	Information Paper No 4 - Privacy Commissioner (Aus) 1995	http://www.privacy.gov.au
Privacy and Biometrics	Ontario Privacy Commissioner, 1999	http://www.ipc.on.ca/english/pubpres/sum_pap/summary.htm
Privacy Framework for Smart Card Applications	Privacy Commissioner of Canada, 1996	http://www.privcom.gc.ca/english/02_05_e_01_e.htm

Biometrics for international travel	International Biometric Industry Association (23 companies from Europe, Asia and Nth America)	http://www.ibia.org/news.htm See "IBIA announces privacy principles". Also see articles on Simplified Passenger Travel Interest Association, set up by the International Air Transport Association (IATA) to promote the use of multi-functional smart cards (or other device) that includes a biometric ID, for international travellers to facilitate customs and immigration controls as well as airline services. See also http://www.simplifying-travel.org/public/news.php3?information[id_information]=37 and http://www.slb.com/smartcards
A brief history of smart cards for US Government		http://smart.gov/information/moore_pp0200/john_moore.htm
Smart Card Industry Association - examples of applications of smartcards around the world		http://www.scia.org/