Privacy recommendation on use of smart cards

Smart card experiments are taking place and being planned in different countries for different purposes. Dr David Flaherty, Information and Privacy Commissioner for the Province of British Columbia (BC), Canada, has produced some privacy recommendations on use of smart cards which may well be applicable elsewhere. This version has been edited omitting specific references to BC law.

My basic recommendation is for a system of voluntary smart cards that permit individuals to choose how to identify themselves at various points in their daily relations in society. In fact, individuals could choose to use the card, freely, for any kind of transaction where identification is normally required today, such as cheque cashing.

The advantage of true smart cards is that they can be adopted for multiple purposes over time, including the following possible applications, each of which would have a separate, segmented portion of the card:

- medical data
- emergency medical information
- anonymous telephone charge card
- credit card/debit card/charge card
- library card
- driver's license.

Personal data would be collected directly from the individuals concerned (when the card was used). Individuals would also have a right of access to all of the data on their smart card and also be able to control whether or not other users access segments of the card.

Summary of recommendations

I want to emphasise that what follows is a package of recommendations that need to be accepted, almost in full, as a package. They are intended as a "coherent" whole. Thus, rejection of one may cause this particular house of cards to come tumbling down.

1. The implementation and ongoing use of ID Cards should conform to **"fair information practices"** recognised internationally.
2. There should be **full transparency** in the implementation and ongoing use of ID Cards. The public must be educated on how identification cards work and what choices they can make.
3. The principle of **finality** must be applied to the conception and implementation of ID Cards. This means that legitimate uses of ID Cards should be established in advance of data collection and data sharing.
4. The use of ID Cards by the public should be voluntary, which means that they be used by **informed consent** only.
5. ID Cards should, in fact, be **smart cards,** where the individual alone can control their use, including authorisation for its use by means of a unique password.
6. Individuals must be able to control access to their own data. Therefore, **passwords** should be mandatory if smart cards are adopted as the basic identity card.
7. There should be a **prohibition on the routine profiling of individuals** based on transaction data, unless there is reasonable and probable cause to do so for law enforcement purposes.
8. There should be **oversight, audit and complaint-handling mechanisms** in the use of ID Cards. The use of ID Cards, from a privacy perspective, should be fully subject to the **oversight of a Privacy/Data Protection Authority.** This means that public bodies would be required to consult with the DPA in advance of seeking new applications of identity cards.
9. The holder of an identity card should be identified uniquely by his or her **digitised photograph, rather than by a unique personal identifier.** Any serial number on the card would be attached to the card and not the holder. Thus, any replacement card would bear the next assignable number, rather than a unique identifier.

Source: Notes for a presentation entitled *Provincial Identity Cards: A Privacy-Impact Assessment* by Dr David H Flaherty, Information and Privacy Commissioner for the Province of British Columbia, Victoria, BC., Canada September 26, 1995 (11 pp.)