Issues in Compulsory National ID Schemes and Related Personal Identification Technologies

Discussion paper presented at the panel

Weatherhead Center for International Affairs, Harvard University

Tyng–Ruey Chuang

May 3, 2004

1 National ID Schemes

A national ID scheme is often compulsory, and it is compulsory in two senses. First, each citizen or legal resident must apply for and receive the ID. You must get one, there is no exception. Secondly, each national ID holder is required to use the ID in certain ways. You cannot get away with it. For example, a citizen may be required to carry his/her national ID at all time, and to present the ID to the authority when it is demanded.

In a country with a national ID scheme, the ID is often required when a citizen is to interact with government agencies. It is used both to identify oneself and to assert one’s citizen rights. For example, one need to present his/her ID when casting a vote in a public election, when applying for one’s passport, and when applying for social welfare, just to name a few. In short, your national ID card is the “root” certificate issued by the government for your identity and citizenship. Other official identification documents, as well as all kinds of citizenship benefit, can only be produced or generated if this root certificate is presented.

I would like to emphasize that a national ID scheme necessarily introduces a nationwide personal numbering system. Each national ID will have a unique ID number, and the ID holder often is to be identified by this number. In some country, for example in Taiwan, the national ID scheme is also an integrated component of a household registration system that is maintained by the government administration. When one discusses issues of a national ID scheme, one also need to consider related issues in the associated personal numbering system as well as the the household registration system.

The national ID and the personal ID number also are used in many societal functions. The situation is not too different from that in the US one often presents one’s driver license (actually the date-of-birth data on the license) as a proof of age when,
for example, buying liquor or tobacco. In Taiwan, for example, one need to present his/her the national ID when opening a bank account or applying for a credit card. The bank and the credit company will even make a photocopy of the ID during the application process. We may say that the usage of national ID and ID number can be non-regulated, unless there are explicit restrictions imposed by the government on their usage.

For an existing national ID scheme, it can become a kind of “legacy system”, a system that was set up years ago but is increasingly out-of-pace in the current society. The urgent need to update the scheme in part, or to re-engineer it as a whole, often is used as a strong argument to introduce new information technologies, especially new personal identification technologies, to the existing ID scheme.

2 Personal Identification Technologies

Personal identification technologies can be grouped into three categories based on how the identification is established. Your identity can be established by what you know, or by what you have, or by what you are.

In the “what you know” category, a priori secret is shared between you and the party to whom you want prove your identity. Once the party is convinced that you know the secret, you are identified. For example, your login-in name and password is the shared secret between you and the computer system to which you want to access. You are identified by your account number and the PIN when doing online banking, etc.

In the “what you have” category, you are identified by a physical token no one else has. The token shall not be easily forged. Whoever has the token will get identified. Examples include car key, house key, etc.

In the “what you are” category, you are identified by characteristics of your biophysic self, like your photo and fingerprint (the photo being the characteristics of your face, and the fingerprint the characteristics of your finger).

Each of the above three categories has its own advantages and dis-advantages which I will not be able to explore fully because of the time constraint today. But let me briefly mention that secret can be leaked, token can be lost, and yourself may change. No personal identification technology is without weakness.

If used properly, technologies from the three categories can be combined to achieve greater security. A such example is a photo ID that require PIN input from the ID holder to be valid.

However, there will always be attacks to break these personal identification technologies, as long as a successful break-in will bring sizable financial gain. Note that the attack is directed to the entire system, not just to a specific personal identification technology. The attackers will work on the weakest link in the system. Some of these attacks can simply be social engineering attacks.

For example, instead of forging an passport and the US visa on it, one can simply buys out a valid passport with a valid US visa already on it. As long as the original holder and new holder of the passport look very much alike, the passport may well be used by both persons.
Sometimes personal identification may be too strong a requirement, and the technologies it uses unnecessarily intrusive, for the intended (social) functions.

For example, when taking out a driver license to prove one is over 21 years old and is allowed to buy liquor, one inadvertently reveals one’s exact age (even the exact date of birth), address, and the driver license number.

3 Issues in Crypto- and Biometrics-based National ID Schemes

As one’s national ID is considered as the root certificate of one’s citizenship, and governmental administrations as well as societal functions often depend heavily on it, it is only natural that multiple personal identification technologies are used together to protect the ID’s integrity. The integrity of a national ID scheme, once it is established, is considered very important to the government, to the ID holders, and to a general extent, to the entire society.

There is a trend to use cryptography and associated computation devices in the implementation of a national ID scheme. Typically this will use a smartcard as the ID carrier. A smartcard is a credit card sized plastics embedded with a computer chip inside. The embedded chip will able to perform integrity check and data verification on behalf of the ID issuer. The embedded chip also have a rather large memory capacity so more personal data can be easily stored in the ID. It is often proposed that digitized fingerprint of the ID holder is stored inside the embedded chip. When the ID is used in combination with a smartcard reader with a live-fingerprint scanner, the embedded chip in the ID can then compare the fingerprint that is just scanned with the one that is stored in the chip. The ID holder is identified only if the two fingerprints match.

There are several issues in such a crypto- and/or biometrics-based ID scheme, from the perspective of ID holder’s rights. First, the data stored in the smartcard is not human readable. Without access to a smartcard reader, the ID holder have no way of knowing if the data in the chip is correct, complete, and without unnecessary annotations. Even with the access to a smartcard reader, still the ID holder has to trust the smartcard reader will indeed reveals all the data in the chip.

Note that the ID holders may be required by law to not tamper with the smartcard-based ID and the associated smartcard reader (think Digital Millennium Copyright Act, DMCA). The ID holder may not even legally own the ID card itself, not to mention the rights to tamper with it.

This can be considered a serious erosion of control about one’s personal data. In addition, the memory in the smartcard is writable. This leads to the possibility that the transaction history of the smartcard ID can be constantly updated in the smartcard memory, and can be released back to some smartcard readers without the ID holder knowing it. By transaction history, I mean the history of the smartcard ID being used; that is, what smartcard readers does the smartcard ID come to contact with, as well as the where and when of the contact. If unchecked, a smartcard-based national ID scheme can be turned into a nation-wide data surveillance infrastructure.

A crypto- and biometrics-based national ID scheme has many social and political
implications. However, only people with sufficient level of information literacy will be able to fully articulate these implications. We shall concern that, being citizens of participation democracies, whether we have sufficient information and opportunity to discuss these issues with our fellow citizens.