## Pervasive Computing

*House of Commons Science and Technology Committee. July 2006.*
**Identity card Technologies: Scientific Advice, Risk and Evidence**

Identity cards will increase the availability of digitised biometric data. Internet service protocols are vulnerable to error and misuse, potentially giving rise to new control errors e.g. inaccurate transactions and security access, or, errors on a much larger scale.

The identity card Bill was passed in March 2006. It is expected that identity cards will be issued, beginning in 2008.
Identity cards will carry biometric data. This will probably be based on face, iris and fingerprint. Intended uses are to:

- prevent or detect crime;
- ensure national security;
- enforce immigration controls;
- secure the efficient and effective provision of public services; and
- enforce prohibitions on unauthorised working or employment.*(sic)*

The plan is to control the registration (enrolment), storage and availability of biometric data.

Fundamental to the utility of this data are:

a) False match rate—the probability that a person's biometric data matches the data of another person. For finger prints and iris scans the probability of deciding a person is someone else has been found to be $1.3\times10^{-10}$ and $5\times10^{-12}$ respectively.

b) False non-match rate—the probability that a person's biometric fails to match their own enrolment template. For finger prints and iris scans the probability of failing to identify the person as themselves would be 1% and 5% respectively.

c) Failure to acquire rate—the submitted image is too poor for the system to make a reliable decision. For face data the rate is close to zero, but for fingerprints and iris scans the rate of failure is currently 1% and 0.5% respectively.

Clearly the risk of matching to someone else is very low, but the risk of failing to prove that you are who you claim to be is quite high. It would be interesting to discover the same statistics for CHIP and PIN and password protection for internet banking.

Comment
Identification errors could lead to safety failings and transactional losses. In our view, once digitised, biometric data is commonplace it will be used in many more ways than indicated in the above list. Identity uncertainty could be reduced but the scope for organised crime and misinformation will be increased, especially if decision mechanisms are supported by internet protocols.

———