Since each identification involves a comparison against the entire set of prior enrolments, error rates for this one-to-many identification search will depend on the size of the database. Can biometrics deliver acceptable levels of usability and security when we're matching individuals against a database of around 50 million? With several thousand applications per day, if the rate of false positive identification is much more than 1 in 1000, the workload of further identity checks would be unmanageable. Thus 1 in 1000 is the target rate for the one-to-many false positive identification error rate. When the identification is made against the entire database, it would involve some 50 million one-to-one comparisons. As a National Physical Laboratory feasibility study on the use of biometrics indicates (http://www.homeoffice.gov.uk/docs2/ feasibility_study 031111_v2.pdf), to obtain this level of performance the false match error probability for one-to-one comparisons (the probability that a comparison between Mr Brown's biometric and an individual database entry results in a false match), ought to be smaller than 1 in 10_{10}.

According to the NPL study, a good fingerprint system might achieve a false match error rate of 1 in 10_5 using a single finger; the false match rate for a single iris is better than 1 in 10_6, while for facial recognition the false match rate is more typically 1 in 10_3. Thus the NPL study recommends that, in order to uniquely identify one person in a population of 50 million, a fingerprint system should use at least four fingers per person, preferably eight; an iris system should use both eyes, and facial recognition could not, on its own, provide a sufficient accuracy of identification.

Facial biometrics could be used as an aid to identity checking for passport holders. In this instance, which is a one-to-one comparison, the relevant usability parameter is the one-to-one false rejection rate [false non-match rate]. SmartGate, a pilot study of a face recognition passport control system at Sydney International Airport, revealed a false rejection rate of approximately 1 in 50. This is reasonably encouraging. However, the SmartGate study was restricted to less than 4000 Qantas aircrew and it is by no means certain that the same results would be obtained when applied to a larger, possibly less cooperative, user base.

Irrespective of the likely error rates for SmartGate-type systems in 'real world' applications, the ICAA's [International Civil Aviation Authority] choice of facial biometric remains controversial - 'a grave error' in the opinion of Professor John Daugman, the inventor of the dominant iris-recognition algorithm.