An Introduction to Biometrics and Large Scale Civilian Identification

RICHARD HOPKINS

ABSTRACT This paper introduces the reader to biometrics and explains how modern biometric technology is used for verification and identification of individuals. It begins by defining the specialist terms used by the biometric industry. It then goes on to consider the difficulties of using biometric technologies in large-scale civilian environments such as National Identity schemes. The paper concentrates on the practical difficulties of accuracy and scaling and considers some fundamental limitations. After establishing that such large scale schemes are difficult to implement, it reflects on how biometric technologies have been adapted and augmented to cope with these challenging situations. The paper concludes by looking at the likely future of such schemes and the likely advances in biometric technology.

Introduction

On the twentieth anniversary of the first computerised biometric identification system, this paper reflects on biometric technology and the progress it has made.

The paper is an updated version of a number of technical White Papers issued by IBM in 1997. Since publication of these original papers, two biometric based National Identity systems similar to the one considered in the original papers have gone live. This updated version of the first two papers reflects the experiences of the author and others in the commissioning of these systems.

What is Biometrics?

The strict definition of biometrics is the science that involves the statistical analysis of biological characteristics. A (slightly) more pragmatic definition is:

biometrics n. The application of computational methods to biological features, especially with regard to the study of unique biological characteristics of humans.
As with many terms, the computer industry has adopted the word and subtly changed its meaning. Biometrics has thus become synonymous with the verification of peoples’ identities using their unique characteristics.

A biometric is something that is used as a means of proving you are who you claim to be, just like a PIN or a password, but the crucial difference is that the biometric is something that is a part of you, rather than something you know. Some examples include your height; weight; the shape of your hand; the pattern of your voice, veins, retina or iris; your face and, most commonly, the patterns on the surface of the skin of your thumbs or fingers; the fingerprint.

**History of Biometrics**

Primitive biometrics such as height have been used to identify people since the time of the ancient Egyptians. Advances in computer technology now mean that the comparison of biometrics can be at least partially automated. Police fingerprint officers across the world now routinely use automated fingerprint identification systems to help them search for and identify suspects.

**A Common Understanding**

Despite biometric technology becoming more widespread, one of the trickiest challenges in the biometrics industry is to find a common language or viewpoint from which to conduct a conversation. Whilst the industry has made a start towards standardisation, the end of the road is not yet in sight. This paper, therefore, begins by establishing some of the key terms. The first thing that needs to be understood is that verification and identification using biometrics are two very different tasks.

**What is the Difference Between Identification and Verification?**

Currently, biometrics are predominantly used for verification rather than identification purposes. The distinction between the terms is often lost and it may be helpful to define them.

**Verification**

Verification by biometrics asks the question ‘Am I who I say I am?’ It works by comparing a previously stored piece of biometric data against an actual physical biometric as read by a scanner. Typical applications for this technology are for gaining access to buildings or for proving entitlement to welfare payments.

Biometric verification performs the same function as a PIN number, password or signature, but as it involves measurements performed on a physical biometric (such as fingerprint or the shape of a hand) it is usually deemed to be more secure, as the physical biometric is hard to copy. Essentially, therefore, verification is a straight ‘one to one’ comparison between scanned and stored data. Typically the application will be tuned to give a ‘yes’ or ‘no’ response to the question ‘Am I who I claim to be?’ to a high degree of accuracy.
Identification by biometrics asks the wider question of ‘Who am I?’ It works by comparing a scanned biometric against a *library* of stored biometric data. In the ideal form of the process each individual entry in the library is compared and the question ‘Am I this person?’ is asked. Identification is, therefore, very like a long series of individual verifications (see Figure 1). Each such verification activity is known as a *match*.

To ensure that an identity is unique within a population, requires that the answer to the question ‘Who am I?’ is ‘You are not known’. Once such an answer has been given, a person’s biometric data can be added to the library of identities. Should they attempt to enrol again, their stored identity will be found. In this way, a biometric based identity system can ensure that a person has *one and only one* identity within the library.

**What does a System Need to do to Establish Unique Identity in Large Populations?**

With small numbers of people, unique identity could be established by a manual process. Information supplied by the person (including biometric data) could be compared by a panel of human experts and a person would be admitted if they found no match to existing personal data in the library.

Such a panel would be capable of deciding absolutely whether a person can be admitted. One can imagine that this process could be automated using computers. Indeed, the biometric industry now claims that specialist automated systems can do a similar job in an automated manner for millions of individuals.

This claim requires careful examination.

**How Many Matches are Required?**

To be completely successful in ensuring that there are no duplicate identities, the system would effectively have to compare a new enrollee against all the people already enrolled in the database. As we have already seen, this means that to uniquely enrol a single individual into a population of 1 million people, 1 million individual verifications would effectively need to be performed. Now imagine a system where an eventual population of 25 million is enrolled at a steady rate of 5 million people per year over 5 years. By the fifth year each
one of the 5 million people enrolled in the last year will have to be compared to over 20 million people already in the system. Over this year over 100 million million matches (asking ‘Am I this person?’) will take place. To give an accurate and unambiguous answer to the question ‘Who am I?’ each one of these comparisons must be correct.

How Long Would This Take?

If we assumed human experts were employed to operate the system and each individual match took 5 seconds for a highly trained person, over 3 million experts working round the clock would be necessary to cope with the workload!

To complicate matters further, each person must be added to the database sequentially. If people were added via parallel streams of activity, duplicate identities could be inserted into the system by each stream. This implies that all 3 million experts would need to co-ordinate their activities and work on the same person at the same time!

Clearly a manual system is entirely impractical to ensure unique identity in large populations.

The Implications of an Automated System

Indeed, the current requirement of governments is for totally automated unique identity systems that can provide quick and unambiguous ‘yes/no’ answers to the question ‘Is this person already enrolled in this system?’ Ideally, no human experts should be required.

This paper considers the implications of this requirement and examines the issues for the biometrics industry in delivering such systems. Throughout the paper, we will examine the case of a 25 million person-unique identity system that must be established within 5 years. Such a requirement is typical of the large-scale projects that are currently underway.

How Fast Would Such a System Need to Be?

The 25 million people need to be enrolled sequentially to avoid possible duplicate identities. If we assume that the final system works every hour of every day, the final system must be effectively capable of performing 3.5 million individual matches (or verifications) per second.

How Big Would Such a System Be?

The biometrics industry has historically been very guarded about the matching performance of its algorithms both in terms of throughput and accuracy. The fastest identification capabilities currently available are for fingerprint matching. These fingerprint matchers perform the individual verifications extremely quickly on specialised hardware, which are in turn supported by conventional computer hardware. The speeds of these matchers are now measured in terms of thousands of matches per second. This means that hundreds of these extremely expensive pieces of technology would be required to support the 25 million unique-identity challenge. Such systems would be prohibitively expensive and extremely difficult to systems manage.
Is System Size the Most Difficult Problem?

Clearly, to reduce cost and aid implementation, ways need to be found to decrease the size of these systems. However, the price/performance of computers effectively doubles every 18 months, so it probably should not be regarded as the limiting factor in implementing large identification systems.

A far more important issue, which inhibits the implementation of large-scale identification systems, is that of accuracy.

Why is Accuracy the Fundamental Problem?

We have already seen that the work that must be performed to establish unique identities for large populations is extensive and requires accuracy. The biometrics industry claims, however, that computers are highly efficient at speeding up the process of identification and can thus make the process practical, cost effective and accurate.

Junk mail, car building robots and monthly credit card statements are testimony to the fact that computers are good at automating large, intensive and repetitive tasks, so on the face of it the claim may appear to be a strong one. However, it is worth examining some of the special factors that affect biometric processing which makes the transition to a totally automated identity solution a challenging one.

The Perfect Circle

A certainly apocryphal story has it that Leonardo Da Vinci was capable of drawing a freehand perfect circle (presumably with his right or left hand). These days a quantum physicist would explain that the way the world is put together does not allow for ‘perfect’ circles. The world and particularly the humans within it are as inexact and imperfect as ever.

The term ‘biometric’ refers to the statistical analysis of biological characteristics. Almost by definition these biological characteristics are subject to change. The use of the term ‘statistical analysis’ itself implies that interpretation of the biometric data is necessary. Biometrics is not therefore an exact science. It needs to take into account different mechanisms for interpretation of data and different environmental conditions when the data was captured.

Take fingerprints, for example, they can be deliberately scarred or mutilated, temporarily damaged by chemicals or distorted by squashing the finger. The capture process of a fingerprint may be via a live scanner or a scan of an inked fingerprint card. Each of these makes the supposedly invariant fingerprint biometric extremely variable. This makes highly reliable identification a very tricky process.

At this stage in this document it may be worth examining just how tricky.

Similarity and Equality

Computers find it very easy to deal with pure equalities. Withdrawing money from your bank account using information read from your cash machine card is an example of a computer being able to easily equate the unique number stored in the magnetic stripe of the card with another unique number within the bank’s systems. Despite the large number of
accounts and card numbers stored in these systems the comparison is easy and straightforward.

Computers find it much harder to deal with things that are similar, but not exactly the same. Ask a conventional computer database to find the account for a person whose name sounds something like ‘Hopkins’ and lives somewhere in Northern Europe and your wait could be considerably longer.

Basically, the task of identifying only the right data in a search, which has elements of uncertainty, becomes more difficult:

- the more similarity there is in the data to be searched
- the more scope for error there was in entering the data in the first place
- the bigger the database gets.

A biometric system which needs to establish unique identities for 25 million people using biometrics is at the extremely difficult end of this scale. Let us consider an example.

**Apples and Oranges**

At first sight it is relatively straightforward to distinguish an orange from an apple as shown in Figure 2. This is especially true when we have access to the real article and can use all our senses to make the judgement.

Life can get harder, however, when presented with a wider selection of pictures or photographs of random apples and oranges of different types as shown in Figure 3. Ask yourself the questions ‘Is this fruit an apple?’ and ‘Is this fruit an orange?’ for each of the fruits shown. Your result will be influenced by your evaluation algorithm (your brain!) and by environmental factors (including whether you are reading this document in black and white or colour).

Imagine the difficulties faced by a computer when presented with the task of quickly distinguishing between 25 million essentially similar and often distorted biometrics.

It is unreasonable, therefore that any biometrics system should be 100% accurate, but just how difficult is it to correctly identify one person in 25 million?
**Rosencrantz and Guildenstern**

In the play *Rosencrantz and Guildenstern are Dead* by Tom Stoppard, the two protagonists find themselves in the unusual situation of having tossed a fair coin nearly one hundred times with each spin landing heads.

We know instinctively that such a run is almost impossible, but just how probable is it? Each individual toss of the coin has an even chance of landing heads or tails (a 50% chance of a head or a tail). To achieve a run of two heads, there is a 50% chance that the first toss will be a head and then a further 50% chance that the second toss will be a head. Overall there is, therefore, a 50% chance of a 50% chance, i.e. a 25% chance of getting two heads in a row. To get three heads in a row the chance would be a further 50% of the 25%.

To understand how improbable 100 heads in a row is, we must multiply our original 50% chance by itself 100 times. The probability of 100 heads in a row turns out to be: 0.0000000000000000008%. This is a very small number indeed!

If we had tossed a coin every second since the estimated moment of the Big Bang, then there would still be a less than a 1 in a billion probability that we would have obtained 100 heads in a row (55 in a row is probably the best we could have expected over this rather protracted period).

**Getting it Wrong**

Using this type of theory it becomes possible to understand why biometric identification in large populations is such a difficult proposition. Looking at Figure 1 again, we can see that establishing a unique identity is like performing a series of verifications or matches.

Each time the system asks ‘Am I this person’, the system can answer ‘yes’ or ‘no’. In addition the system could be right or wrong in its comparison (shown by the and ). These four possible outcomes are labelled (1)–(4) in Table 1.

Outcome (1) means that the system has correctly found a duplicate identity within its database. The system would then rightly refuse the enrollee the additional identity they have requested.

Outcomes (3) and (4) are both wrong answers to the question ‘Am I this person?’ They happen when the system makes an incorrect biometric comparison between the person being enrolled and one of the people already in the system. Unfortunately the identification system *as a whole* will make a mistake in its decision on whether to grant a unique identity if *any one* of the 25 million individual ‘Am I this person?’ decisions results in either of these outcomes.
Table 1. Question: Am I this person?

<table>
<thead>
<tr>
<th>Answer:</th>
<th>(System is right)</th>
<th>(System is wrong)</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES you are</td>
<td>(1) I am identified</td>
<td>(3) I am wrongly identified</td>
</tr>
<tr>
<td>NO you are not</td>
<td>(3) I am not this person</td>
<td>(4) I am not identified</td>
</tr>
</tbody>
</table>

Within the context of an identity system, outcome (3) is known as a false positive. This is because the person applying for a new identity will be incorrectly refused as the system will say that they already have an identity when actually they have not. The person has been falsely rejected. A human investigator would then need to intervene to check additional details (such as a photograph) to understand whether the supposedly duplicate identity is a real duplicate or not. In the case of outcome (3), the human investigator would have to overturn the system’s decision.

Outcome (4) is a false negative. This is because the system will accept the enrollee into its database even though that individual already has one or more identities within the system. This outcome is effectively the chance that a dishonest person could ‘fool’ the identification system into giving them another identity.

To ensure that a person has a unique identity in a population of 25 million people, the equivalent of 25 million of these individual verifications must occur. This implies that for a genuine applicant without an existing identity in the system, outcome (2), and only outcome (2) must happen 25 million times in a row.

We have already seen that a mere 100 events happening in a row can mean that the resultant outcome is highly improbable. How good must an identification system be at answering ‘Am I this person?’ to ensure that a person is unique within a population of 25 million people?

The answer is quite simple, to ensure that a person is unique, the system must be 100% accurate and never make a false comparison. We have already established, however, that this is an unreasonable claim for a biometric based system (please see the subsection Apples and Oranges above), so in the next section we examine what accuracy we might expect.

Ninety-five per cent Accuracy

As we alluded to in the subsection The Perfect Circle, the likelihood of a biometric system that does not make mistakes is close to non-existent. For example when using fingerprints, inaccuracies introduced by the human environment (such as sweat, dirt and various distortions) and chance similarities between biometrics within the database are capable of distracting even the best matching algorithms.

A biometric system will hopefully be right for a high percentage of the time, but in the biometrics industry even getting it ‘right’ is a term that needs some explanation.
Balancing Strictness and Leniency

In Table 1 we saw how each simple match could have four possible results. Two of these results were errors; the false negative (4) and the false positive (3). Biometric systems attempt to make both these errors as small as possible, but every biometric system can be made either more strict or more lenient by balancing these errors against one another.

As a biometric identification system is made stricter, the chance of being falsely rejected becomes higher (i.e. there are more false positives), but the chance of being falsely accepted becomes less (fewer false negatives). If the system is tuned to be more lenient, then the chance of being falsely accepted grows, but the chance of being wrongly rejected diminishes.

Tuning the False Positives and Negatives by Application

This capability is often used to make the same biometric identification or verification system meet the specific requirements of its environment or application.

As an example, it is worth looking at two different applications.

Consider a situation where money is being collected from a bank’s cash machine with a biometric being used for authentication. In the cash machine, the biometric algorithm would be tuned to provide a good level of security, but would not inconvenience the customer by rejecting their biometric too often.

In contrast, consider a biometric being used as an authentication mechanism for control over a nuclear power station. In this case, the system would be tuned to provide a much higher degree of security rather than convenience. This could possibly sometimes mean requiring more than one attempt to authenticate a person’s identity.

Choosing the Right Operational Characteristics

By trading off the frequencies of false positives or false negatives it is possible to tune a system to be either lenient or strict. If we wish to fully define the requirements for our 25 million person identity system we will also need to define the operating accuracy characteristics for the system in terms of acceptable levels of false positives and false negatives.

One Possible Scenario

Let us therefore consider a system that has the following apparently reasonable characteristics:

- supports 25 million people
- catches 95% of the people who try to gain false identities
- only half a million rejections need human intervention over the five years.

Such a system would be a deterrent to those who might attempt to gain duplicate identities, but would not be so strict as to inconvenience the genuine applicant or involve the clerks operating the system in making too many decisions.
Table 2. Question: Does this scanned biometric match this entry in the database?

<table>
<thead>
<tr>
<th>Answer</th>
<th>(System is right)</th>
<th>(System is wrong)</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES, it does</td>
<td>(1) true match</td>
<td>(3) error: false positive</td>
</tr>
<tr>
<td>NO, it doesn’t</td>
<td>(2) not a match</td>
<td>(4) error: false negative</td>
</tr>
</tbody>
</table>

These operating characteristics have been chosen by the author to reflect the kind of expectations that many governments have for large civilian identification systems.

Let us consider some of the implications of these requirements.

What are the Accuracy Characteristics of this System?

Let us recap on our original Table 1, but this time we shall use the formal terms we have defined and represent the same information as Table 2.

Within an identification system that needs to support 25 million people, the equivalent of up to 25 million of these comparisons must be performed to ensure that an identity is not in the database and is therefore unique.

False Negative Rate

If we assume there is a previous identity in the system, we have asked the system to find it 95% of the time. This could be conversely reworded as asking for a system which only falsely accepts a duplicate identity 5% of the time.

Looking back at Table 1, every time we compare two matching biometrics (i.e. duplicate identities), the system can produce one of two outputs. The match is either found (1) or not (4). In this regard, the size of the database becomes irrelevant. If there is only one previously enrolled identity already in the system for the person who is attempting to re-enrol then there is only one chance of getting the decision right or wrong.

Even if the database grew to 100 million identities, there would still be only the single chance of getting it right or wrong.

The false negative rate of a system is, therefore, independent of the database size. This means that for the individual comparison or match, the false negative rate can be the same as the overall system, in this case 5%. This means the system must make a correct decision 19 times out of 20.

Even given the unpredictable nature of biometrics, this seems a more than reasonable capability to ask for, so let us now consider the false rejection rate that we have stipulated.
False Positive Rate

If we now assume that there is not a duplicate identity in the 25 million identities in the system, we can now consider the chance of the system falsely rejecting someone (i.e. not allowing them to enrol their identity when it should).

For every comparison where a match should not be found, the system can respond with outcomes (2) or (3). In this example we will be making 25 million of these comparisons in a row.

We have previously stipulated that the system should only require human intervention in half a million cases out of 25 million. This means that the false reject outcome (3) should only happen 2.5% of the time. Conversely, we can think of this as a requirement that states that for 97.5% of all the identifications the system does, outcome (2) (the right outcome) should happen 25 million times in a row!

This feels very unlikely, but how unlikely is it?

Using the same mathematics we used for the coin tossing experiment we can calculate how reliable an individual decision must be (between outcomes (2) and (3)) to allow the system to be right 97.5% of the time when it has to perform 25 million of these decisions.

As it turns out, the answer is that the system can only afford to make a mistake once in every thousand million comparisons.

Even fingerprint, the most mature of biometric identification technologies, has not aspired to this level of accuracy.

At this point it is worth reiterating the point we made earlier: biometrics is not an exact science. By asking this relatively new technology to deliver a decision-making capability that hardly ever makes a mistake, we are asking it to deliver a precision that may well be unattainable.

A Review of Our Requirements

What seemed at first to be a perfectly reasonable request: ‘establish unique identities for 25 million people within 5 years using biometrics’ now seems unreasonable. To recap, the underlying requirements of this system can now be worded:

- implement a system that performs 3.5 million biometric comparisons per second

At this throughput ensure that for each comparison this system makes:

- only 1 in 20 of true matches are missed
- only 1 in 1,000 million non-matches are wrongly construed as matches.

Whilst our original requirements seemed reasonable, these (which are effectively the same) appear less so. What can be done to make these latter requirements more reasonable without sacrificing the first set?

How can such Demanding Requirements be Met?

Having established that these requirements are difficult, we can now look at how the biometric industry has gone about meeting them. To ground this understanding, the paper will look at implementation issues on real systems. Whilst other biometrics may also be
suitable for large-scale civilian identification, the author is only aware of two such systems which have begun enrolling. Both are based on fingerprint technologies.

A Brief History of Fingerprinting

Fingerprints have been used for identification purposes for hundreds of years. The first recorded use of fingerprints was in ancient China when letters were proven to come from a particular person because the wax seals were embossed by the fingerprint of the sender.

In the seventeenth century it was noted that each person’s fingerprints were different and could be classified into patterns such as arches, whorls and loops. By the late nineteenth century, law enforcement agencies started collecting fingerprints of criminals. During the 20th century, this collection of fingerprints became routine. Now, at the end of this century it has become possible to automate the fingerprint identification process using computers. It is these systems that this paper examines.

A Background to the Industry

The fingerprint identification industry is a highly specialist field that has coined its own name: AFIS (Automated Finger Identification System). As might be expected from the brief history above, AFIS has its roots in law enforcement and AFIS systems are designed to aid and partially automate the tasks of the fingerprint officer.

Now, 20 years after the first AFIS successful installation, there are many vendors and the law enforcement AFIS market could be considered to be mature.

Today, however, there is a new market emerging called civilian identification. This market has very different requirements, but the law enforcement AFIS vendors are attempting to adapt their systems to meet them.

This paper looks closely at these attempts and explains the techniques being used and some of their limitations.

To understand these complex topics, however, the reader needs to understand a little of how AFIS systems work. Fortunately, despite the wide variety of vendors, almost all the systems work in essentially the same way. In the next section we examine how.

How do AFIS Systems Work?

Computers find it difficult to cope with biometrics in their raw form. Biometrics can be deformed or damaged through environmental or deliberate abuse. This makes quick comparisons between two different pictures of the same fingerprint very difficult as the pictures may look quite different.

In AFIS systems it is expected that the pictures of the fingerprints captured for identification or verification purposes will be rotated and distorted from the original pictures used for enrolment. Like two peoples’ television sets, these pictures are also usually at different contrast and brightness levels. In addition, temporary scarring or degradation of the fingerprint may change the features of picture significantly. The combination of all these difficulties usually means that the two pictures of the same fingerprint being compared are far from identical.

Comparing similar but not identical pictures was considered earlier (please see *Apples and Oranges*). In order to compare similar fingerprint images (i.e. two different pictures of
the same finger) computers attempt to reduce the similar images to mathematical elements that can be regarded as equal or identical.

Reducing Pictures to Information

This reduction process is like the difference between a year’s worth of bank statements and a household budget derived from them. The second is purely derived from the first, but the second contains information that is easy for the human brain to understand.

The commonality here is the reduction of raw data to numerical information that is much easier to ‘process’.

‘Thinning’ Images

This process of reducing complex and slightly similar ‘pictures’ of biometrics down to much simpler mathematical elements is common across the biometrics industry.

In terms of fingerprint images, the first stage in this process of simplification is called ‘thinning’. Thinning takes the original fingerprint image that contains greys and environmental noise down to lines made up of small black dots on a pure white background. Each of these lines is a line or friction ridge on the fingerprint being examined.

The pattern of these ridges is the thing that makes each fingerprint different.

In the process of thinning, the original complex image now looks much simpler and is therefore easier for the computer to analyse. The concept behind the process is that the amount of data has been reduced whilst the information remains. In this case the information is the ridge pattern which distinguishes one fingerprint from another.

Minutiae

Using the thinned image, the computer can examine the individual lines within the fingerprint and identify the points where the lines (or ridges) diverge or when they stop. In the AFIS industry these points are known as bifurcations and end points respectively.

Collectively these features are known as minutiae and effectively reduce the data of the thinned image down to nothing more than a series of points. The arrangement of these points is just like a series of dots on a page of paper or stars in a constellation. Just as the ridges were unique, the pattern of the minutiae is also unique to the fingerprint.

This is a further stage in reducing an originally complex image down to information that is easily understood by a computer. By this stage, most of the complexities of the original image have gone. The effects of contrast, brightness and noise, which we identified before, have been largely eliminated.

These dots or minutiae are effectively a purely mathematical description of the fingerprint (just like some points on a graph).

Whilst the minutiae positions are the most important features of the fingerprint, once the minutiae are determined, the AFIS often goes on to record additional data about these points. This information depends very much on the individual AFIS system but usually includes the direction of the ridge at the minutia point and often includes the number of friction ridges between pairs of minutiae (known as ridge counts). This is recorded because the accuracy of the matching system increases as more minutiae and related information is accurately extracted.
Within a biometric system, the minutiae data is often around 1,000 times smaller than the original image data.

Whilst the arrangement of dots extracted from two different images of the same fingerprint will not be exactly the same, the information is smaller and easier to process and the similarity between the minutiae is much greater than the similarity between the two original images.

The contrast between the complex grey fingerprint image and the simplicity of the minutiae can be clearly seen in Figure 4.

**How do AFIS Systems Compare Minutiae?**

Even when a fingerprint is reduced to a few hundred pieces of information, there is still a lot of work for a computer to do to compare the arrangement of patterns of minutiae (especially if extra information like ridge counts has been recorded). The pattern matching process has to compensate for rotation of the pattern and for rogue minutiae.

Rogue minutiae are points that have been selected by the computer either in the search or original image that are not real or permanent minutiae. This means that the rogue minutiae will not appear in both images. This makes accurate comparisons between patterns of minutiae much more difficult as the patterns become increasingly similar rather than identical.

The comparison or matching process, therefore, involves complex manipulation of the two sets of minutiae to measure how similar they are. After the comparison has been made, a score that indicates the strength of the match is issued by the matcher; the better the match, the higher the score.

Because the system must deal with similarity measurements rather than equalities, a single comparison is still a large amount of processing for a computer to do quickly and reliably.

Only a hundred or so of these comparisons per second could be carried out on conventional computer hardware (such as a modern IBM PC). To enable thousands of matches to be performed per second, AFIS vendors use specialised computer chips to accelerate the comparison process.
What Happens After a Match?

The matching process outlined above results in a score for each individual match or minutiae comparison. What happens with this score depends very much on whether this is a law enforcement or civilian fingerprint system.

For the purposes of the rest of this paper, it is very important to understand some of the major differences between law enforcement AFIS requirements and civilian AFIS requirements.

Law Enforcement AFIS Systems

Law enforcement AFIS systems are used by fingerprint officers to enhance their productivity. They are used to compare fingerprints that are suspected to come from offenders (known as latents) to a database that contains the ten prints of known offenders. These latents are usually taken from crime scenes or documents.

Just as we outlined above, the systems automatically extract minutiae for the prints to be searched for or enrolled onto the system. The fingerprint officer may then check and adjust these minutiae and their associated information to ensure that the computer has made no errors in determining them.

A search is then performed on the AFIS database. It is usual for this search to be restricted by the fingerprint officer to a portion of the database based on additional information about the searched for fingerprint. Usually only a few per cent of the full database is searched.

This additional information may include geographic data about where the print was found or a human assessment of which finger the latent comes from. This technique of restricting the search to specific areas of the database is known as filtering.

If a filtered search does not find a match, then the whole database may be searched using what is known as a ‘cold’ search. This takes much longer and uses far more system resources, but is more certain of finding possible matches.

Law Enforcement AFIS Results

The scores from individual matches are recorded during the search. Typically a threshold or hurdle is set and matches that score on or above this threshold are recorded in a list. This list is then ranked according to the strengths of the individual matches. The most likely match appears at the top of the list.

It is not unusual to have many potential matches to consider in this list which is known as the candidate list.

The original fingerprint images of these potential candidates are then retrieved and the fingerprint officers perform a manual investigation of these images against the latent image. If one of the candidates in the list is judged to have the same print as the latent then the fingerprint officers can be satisfied they have found a correct match in a fraction of the time than they would have been able to using a manual search process alone.

Civilian AFIS Systems

Civilian AFIS systems are quite different. Their task is not generally to identify an unknown person, their primary task is to ensure that a citizen has one and only one identity. As we discussed earlier, in large populations this is a very difficult task.
The first example of civilian fingerprinting took place at the start of this century when railway workers were fingerprinted to ensure they only collected one pay packet.

Nearly one hundred years on, we are looking at the same kind of problem (establishing one and only one identity per person), but this time using computers to prove uniqueness for much larger populations.

It is important, however, to understand that civilian AFIS is operationally very different from law enforcement AFIS. First, the fingerprint officer needs to be replaced by a clerk. The clerk may have had cursory training in how to use the system to capture fingerprints, but will not be a fingerprint expert. The capture process therefore needs to be automated. Checks on quality of image and minutiae extraction cannot rely on human intervention and must be made as far as is possible by the computer.\textsuperscript{5}

\textit{Civilian Matching}

The matching process too is quite distinct both in terms of the scale of the problem, the format of the results and the accuracy that is required.

\textit{Database Size}

Most obviously, the size of the database is likely to be very different. An identity system for a country needs to contain every citizen. A law enforcement system for a whole country (and many are regional rather than national) usually only contains known offenders. Hopefully, the number of known offenders is only a small proportion of the total civilian population! This means the law enforcement systems are generally substantially smaller than civilian systems.

Law enforcement AFIS systems normally support a population in the order of hundreds of thousands of individuals and a few million prints (each person has 10 prints stored in the system). Each search usually only penetrates a few per cent of that database (about 300,000 prints).

Civilian systems like the one we are considering have much larger populations and the searches must penetrate a larger percentage of the database. Many customer requirements have suggested filtering the database by sex only, which suggests that approximately 50\% of the database is searched to determine a unique identity. On a 25 million person system, this is a minimum of 12.5 million prints per enrol (over 40 times bigger than the average criminal AFIS search). In addition, customers often want two prints to be taken from each person to enhance the accuracy of the system or to meet their legislative obligations (please see \textit{More Prints} later in the paper). This means that despite allowing filtering by sex, the system still has to search up to 25 million prints per enrol.

\textit{Civilian AFIS Results}

It is not just the scale of the matching which is very different, however. The throughput of enrols for a civilian system that enrols 25 million people in 5 years is about 15,000 new people per day. If investigators were presented with candidate lists of, say, five possibilities for each of these people, then the manual effort per day would be immense. If each candidate check required one minute of effort, then over 150 fingerprint officers would be required to support the system!
What is actually required is a system that can give a ‘yes’ or ‘no’ answer to an enrolment request most of the time. Earlier we suggested that the system should produce a correct ‘yes’ or ‘no’ response for 95% of enrols. This means that a candidate list is only produced in one out of every 20 enrols. The remainder of the time, human intervention is not required to decide whether a person is really in the database or not.

Using the same basic probability theory that we used before, we can calculate that if we demand a ‘yes/no’ response in 95% of cases, then in more than 98% of the remaining 5% of cases only a single name is suggested!

Each day an operator will need to make around 750 ‘yes/no’ decisions. These decisions are to determine whether a potential match found by the computer is actually a real match. This is a simple ‘yes/no’ decision for an operator to make which could be made on an examination of the photographs and/or fingerprint images of the applicant and the possible match.

The operator would only be presented with more than one possible matching candidate for an applicant about fifteen times a day!

The investigative workload associated with a system that meets our accuracy requirement is therefore hugely reduced. A system which achieves ‘yes/no’ accuracy 95% of the time is capable of being supported by a single fingerprint specialist.

What is the Difference in Accuracy?

It is not intuitively obvious what improvement in accuracy is required to move from today’s AFIS systems (searching on average 1 million prints) to one that searches many millions of prints. This increase in accuracy must also be combined (as we saw above) with the leap in accuracy required to jump from a system that produces candidate lists to one that gives correct ‘yes’ and ‘no’ answers almost all the time.

Using probability theory we can, however, calculate the accuracy ‘jump’ required. Let us consider a system which is representative of the current state of the art AFIS system. This system has the following characteristics:

- average search size of 1 million prints
- candidate list of no more than 3 entries
- 97.5% certainty that any true match will be in the top 3 entries in the list.

The required false reject accuracy for a single comparison in such a system turns out to be about 0.000006%. This means that the system wrongly decides that a match has been made once every 1.6 million or so comparisons. This sounds quite accurate.

Let us now compare this accuracy to that required of a typical civilian system. For this system we have assumed the following characteristics:

- average search size of 25 million prints
- two prints searched per enrol
- no candidate list in 95% of cases.

The required accuracy for a single comparison in this system is actually around 0.000001%. The minutiae matcher can only afford to make a mistake about once in every 1,000 million comparisons! This is clearly a far more demanding target than the previous one. The matching accuracy in the typical civilian system must be over 600 times more accurate than the typical AFIS system installed today.
Supercomputers

As we have seen, the system which can enrol 25 million people in 5 years needs to be capable of making millions of individual minutiae comparisons or matches per second. Can current AFIS technology deliver this kind of throughput?

The very best AFIS minutiae matching technology in the market is based on specialist high-speed processors. Whilst these processors are expensive, they allow minutiae comparisons to be made at very high speeds. Each processor, however, is only capable of a few thousand comparisons per second. To meet the requirements of our challenge we will need literally hundreds of these processors. Unfortunately even the largest supercomputers in the world only have a few hundred processors, so the co-ordination and systems management challenges of a system with literally hundreds of processors would be unexplored territory. Such a system would also be prohibitively expensive!

Existing AFIS v. Civilian AFIS

At this point it may be helpful to the reader to draw up a table to compare the gulf between the typical capabilities of existing AFIS systems and the emerging customer demands of the civilian marketplace.

Table 3 represents the capabilities of three different systems. The first column gives an indication of the capability of a typical law enforcement AFIS system installed today. The second column looks at what the latest AFIS technology is typically capable of. The third column is a summary of the civilian AFIS requirements we have already discussed.

The final column is the most revealing. It highlights the gulf between the normal AFIS capability and the civilian requirement we have defined. In almost every characteristic, the AFIS system needs significant enhancement to meet the needs of the civilian marketplace.

This is particularly true with regard to accuracy and throughput (matches per second).

There is clearly a gap between current capability and the civilian requirement. The rest of this paper looks at how these law enforcement AFIS systems are augmented to bridge this gap.

How Can AFIS Systems be Improved to Meet Civilian Requirements?

The AFIS industry has come up with a number of mechanisms to help their systems scale beyond the basic limitations of their minutiae matching technologies.

The three most important of these mechanisms is known as filtering, classification and expert matching. Each of these techniques is discussed in greater detail below.

Some of these mechanisms are already in use to support the ‘state of the art’ requirements we have just looked at.

Each one of these techniques has its own disadvantages or carries with it an implicit compromise. As the use of these techniques expands to meet the extended requirements of civilian AFIS these compromises become more pronounced and noticeable.

The next section of this paper examines the impact of these techniques on large systems.

Filtering

The easiest way to reduce the capability gap shown in the far right hand column of Table 3 is to use filtering.
As we previously defined, filtering uses data unrelated to the fingerprint (such as the sex of the enrolee) to divide the database into separate chunks. These chunks can then be searched separately.

AFIS vendors usually recommend filtering by sex, but sometimes also recommend filtering by age or other characteristics such as height.

### Advantages of Filtering

The reader may well be asking ‘Why should AFIS vendors want to use filtering?’ If an AFIS vendor’s business is to sell fingerprint-matching systems, then surely using filtering will reduce the size of the AFIS systems and therefore ultimately shrink their business.

To answer this point, let us compare our original requirement for a unique identity system for 25 million people to a new system that supports the same numbers of people, but allows filtering by age and sex so that only a quarter of the database is searched on average.

The original accuracy figure required was for the matcher to only give a false match in 1 in a 1,000 million matches. If we filter to 25%, this figure drops to about 1 in 250 million matches, or about four times less accurate. Clearly this is only a small contribution towards meeting our target of making existing systems 1,500 times more accurate, but the gulf has now dropped to about a 400 or so times improvement.

In addition, the number of matches to enrol an individual has dropped from 25 million to just over 6 million. This brings existing AFIS systems much closer to potentially meeting the throughput targets for a civilian system.

Clearly filtering is an attractive proposition to AFIS vendors as it enables technologies less accurate, and slower technologies than the business requirements demand, to be implemented when otherwise they could not be.
It therefore expands the AFIS marketplace and reduces the AFIS system sizes making them more cost effective.

At this point, the reader may well ask ‘Why can’t you just filter down to a few percent, just like a criminal system? That would make a civilian system many times easier to implement.’ This argument is covered next.

The Downside of Filtering

Filtering is like being challenged to complete any one of 20 different 50-piece jigsaw puzzles. If the pieces are in 20 separate boxes, then the task is extremely simple, you simply choose a box and put the jigsaw together quickly. A 50-piece jigsaw puzzle is no problem at all!

If, however, the pieces are mixed up in a single box of a thousand pieces, then the job of completing the puzzle is much more onerous.

The worst situation, however, is when a handful of pieces from each box have been mixed in with the other boxes by a malicious challenger.

It is impossible to know whether the specific piece you are looking for is in the right box or not. To be certain to find the piece, you have to search all the boxes.

This is an analogous to a civilian identity system where sex, age and region are used to filter a national identity database down to 5% or so.

Those who wish to gain more than one ‘unique’ identity simply lie about their age (possibly using false documents) or travel to an adjoining region or regions. Each chunk of the database potentially contains a separate ‘unique’ identity for a single individual.

In this example, up to 20 ‘unique’ identities could be issued!

To ensure that there could be no duplication of identities across ages or regions, the system would have to periodically compare each person in each chunk of the database against all the people in all the other chunks. But this is exactly the same problem we were trying to avoid in the first place!

Filtering therefore requires a business decision to be made. A judgement must be made between the overall feasibility and cost of the system vs. the impact of people being able to obtain duplicate identities.

If filtering is used to reduce the size of the AFIS and it is easy to provide false information to obtain duplicate identities, then the whole reason and business justification for the identification system is compromised.

Filtering is, therefore, almost impossible to implement successfully on a civilian unique identity project. For this reason, it is the opinion of the author that filtering (other than possibly by sex) is not suitable for unique identity systems.

Classification

Classification is a much harder technology to assess with a view to its suitability for use in civilian unique identity systems.

Classification has its roots in the early days of fingerprint identification when all comparisons were done using a manual process. Even for a fingerprint expert, the careful manual comparison of two prints is a laborious process. Manually comparing against all the prints in a database to ensure a single person’s unique identity quickly becomes impractical and expensive.
In 1901, Edward Henry came up with a partial solution to this problem with a scheme that allowed prints to be classified into different groups according to their pattern. These patterns have such names as loops, whorls and arches, with many subdivisions within the groups.

This allows a manual search to concentrate on a small section of the overall print database allowing matches to be found more quickly and with less effort. True matches can be missed because prints can be wrongly classified, but in the case of manual systems, there is a clear choice to be made between using classification and being able to find a good proportion of matches relatively quickly, or not using classification and taking many days to find all the matches.

Needless to say, law enforcement agencies which operate manual fingerprinting systems generally make extensive use of classification and filtering.

**Computers and Classification**

Many AFIS vendors have attempted to do the same feat with computers. By getting the computer to automatically subdivide the prints into classes, the fingerprint database can be divided into ‘bins’. Each bin contains fingerprints of a certain class.

At first glance this seems like filtering without the drawback that people can lie about the information that subdivides the overall database—the system uses the fingerprint itself to determine the bin into which it should be put.

Classification, however, needs a closer examination as this intuitively simple scheme turns out to be quite complex to implement.

**The Hardest Jigsaw Puzzle in the World**

Imagine a jigsaw puzzle with 1,000 pieces. The picture you are presented with is shown in Figure 5. You are challenged to put the puzzle together within an hour. How would you go about it?

Most people start with the corners. Assuming the jigsaw is a rectangle, the corners are the only four pieces that have two straight edges. They are distinctive and easily discernible. The bottom right corner is the only one that is green, so that is the first piece that is laid on the table. After the corners most people move on to the edges. Edges are easy to spot too because they have a single straight edge. Now, there are likely to quite a few edge-pieces (probably over 100), so you might separate them out into a pile, and then subdivide that pile according to the colour of the edge piece. This often allows the complete edge of the jigsaw to be built (its obvious where the green and orange bits go for instance).

The centre part of the jigsaw is trickier. Now there are no hard edges to consider and there are still well over 800 pieces left.

The experienced puzzler then tends to find distinctive areas of colour in the picture. The picture in the example makes this relatively easy, there are strong areas of red, green, orange and yellow to make the most of. Small piles can be made of these pieces and they can be slotted in reasonably easy.

Now comes the tricky part. The remainder of the pieces is not a particular colour at all.

Of the remaining 500, many are very dark shades of different colours or they are an apparently random mixture of colours. It is very hard to tell them apart. It is even harder to put them in groups or work out where they go on the jigsaw.
One the whole, the best thing to do is to try and separate them into piles on the areas on the jigsaw where they might fit.

If you have got excellent colour vision, that might help, but the picture on the box may have faded due to exposure to sunlight, so the task is made more difficult.

So far we have instinctively put the jigsaw together by going for the most distinctive pieces first and then working down a hierarchy of distinctiveness. At this point, our approach has effectively broken down as we are now likely to start making mistakes in putting the pieces into piles. In addition, when we look for specific pieces, we are probably going to need to look through most of the remaining piles to make sure we find it (these piles contain 500 of the original 1,000 pieces).

Why a Lesson in Jigsaws?

As the reader may have guessed, the parallel I am drawing is between classification schemes in AFIS systems and the approach we have just taken with the jigsaw.

Strongly characteristic fingerprints (the equivalents of corners, edges or small areas of strong colours) are easy to classify and find. For fingerprints these are prints that look like archetypal whorls, arches and loops. Just like the jigsaw, however, these strongly characteristic bins are typically small.

Also, as in our jigsaw example, the characteristics of many of the prints (or pieces) are generally more obscure. Most prints have the characteristics of more than one of the typical patterns (like the multitude of ‘dark’ pieces in the puzzle).

As we have discussed before, computers find it easy to deal with mathematical equalities but difficult to deal with similarities. In the detailed matching process, minutiae allow us
to reduce similar images to information that is amenable to mathematical comparison. In classification, the \textit{similarity of the image} becomes all important. It is exceptionally difficult for a computer to reduce this holistic concept of \textit{pattern} to a reliable mathematical description.

This means that for the large proportion of obscure prints which could fall into a number of bins it becomes easy to make a wrong classification decision if the bins are small. If the bins are larger then there is a greater chance that the right one will be selected. Large bins, however, mean that we end up searching a large percentage of the database, which is exactly what we were trying to avoid!

At this point it is worth remembering that if we make an incorrect classification decision at enrol or at search time, a duplicate identity would not and might never be found. This, of course, compromises the justification for installing the system in the first place.

On the whole, therefore, classification can be used to partition the database as long as we are prepared to sacrifice some accuracy and let some duplicate identities into the system. It is a careful balancing act: the less ambitious we are with classification (e.g. searching about 35\% of the database on average by classification would not be unreasonable) then the less effect it will have on reliability.

Indeed, if we are prepared to allow a few percent more false negatives (and therefore allow the chance of some more duplicates), we can divide the database into relatively small areas using the combined classification of the two prints. This might split the search down to around 10–15\% of its original size (the cross classification of two prints would provide classification of approximately 35\% of 35\%).

Taking the technique to its extreme, however and attempting to classify a search down to a few percent of a database when the system is intended to look for duplicate identities is fraught with difficulties with large numbers of potential matches not being checked and duplicate identities potentially being inserted.

\textit{Combining Filtering and Classification}

If we conclude we are happy to allow male/female filtering and 12\% classification, we have reduced our original requirements from 1 in a 1000 billion accuracy and 7 million matches per second down to around one sixteenth of their original levels.

This is not enough, however, to reassure ourselves that the existing systems will scale to provide 25 million unique identities in 5 years as the improvements we were looking for from the existing systems were 600 and 140 times respectively.

What else could the law enforcement AFIS vendors do to get the remaining boost in performance they need?\textsuperscript{6}

\textit{More Prints}

One approach might be to take more than two prints from each applicant. This elongates the fingerprint capture process and increases the AFIS size. This in turn unfortunately increases the cost of implementing and operating the system.

On the positive side, however, matching more than two prints per applicant allows the system to make a more accurate matching judgement based on more information. For example, the chances of four prints being wrongly matched with the equivalent four prints from a different person is extremely unlikely.
Adding these additional prints to the system, however, increases the cost and required throughput. As the required throughput for a single finger 25 million person system is 70 times greater than current systems, adding extra prints also adds risk to the implementation of the system.

Finally, using more than two prints is often operationally unacceptable to the government buying the system. For example, many countries already have a pre-determined number of fingerprints that are captured for their existing national identity systems (usually two or ten). Some countries even have legislation that mandates the number of prints that must be taken.

The combined impacts of increasing system cost, risk and the changes that may be needed to existing legislation or procedures often makes using more than two prints an impractical proposition.

**Expert Matching**

The final potential solution to the accuracy problem is an ‘expert matching’ system.

An expert matching system performs a similar task to the people who inspect the candidate lists as described earlier in the paper.

These systems use a variety of difficult and computer intensive techniques to perform slow, but very accurate matches between individual fingerprint images rather than minutiae. To continue our jigsaw puzzle analogy, consider the situation when you are attempting to complete an area of a given colour, but you are looking for a specific piece. The usual approach would be to quickly select the likeliest candidates based on their overall colour and put them in a separate pile. You could then examine each of these pieces in detail to see whether it was the piece you were looking for.

Expert matchers do a job just like this detailed comparison of a small number of pieces. They are used as the second stage in a two stage matching process. The conventional minutiae matcher (as described earlier) is used to create a candidate list of possible matches. From an accuracy viewpoint, this is much easier than providing a ‘yes/no’ response.

The expert matcher is then used to evaluate the contents of this candidate list.

**Making Minutiae Matching Easier with an Expert Matcher**

As we have already seen, candidate lists get longer as minutiae matchers get less accurate.

One of the key drivers of the original accuracy requirements in Table 3 was that for 95% of the time we wanted the matcher to respond ‘yes/no’. A ‘yes/no’ response is equivalent to a zero length candidate list. This makes the matching requirement a very difficult one to meet (the minutiae matcher could only make a mistake once in 1,000 million comparisons).

Alternatively, however, if we mandate that in 95% of cases we want a candidate list of no more than three people, the accuracy requirement for the minutiae-matching system can be significantly reduced. These candidate lists can then be passed through the expert matcher to qualify them to provide a ‘yes/no’ response.

The expert matcher will add its own inaccuracy to that of the minutiae matcher, but for the moment we shall assume that the expert matcher is highly accurate and therefore the error it contributes is negligible.

When we calculate the new minutiae-matching accuracy requirement for this two stage system, we find that the error rate is 0.0000025% (i.e. the system can afford to make a...
mistake about once every 40 million comparisons). This is only about 25 times more accurate than currently implemented systems, which is far more reasonable than the 600 times more accurate capability that we originally wanted.

Clearly, expert matchers potentially have an important role to play when the minutiae matcher is insufficiently accurate to give a ‘yes/no’ response.

What Population is Possible?

To determine the limits of what is currently possible using law enforcement AFIS technology, we shall assume that the AFIS vendor decides to use a reasonable mix of the techniques we have examined to build a system. If those techniques were used, what could be accomplished? One possible scenario is given in the following list:

- 50% filtering (male/female)
- two fingers
- 2% classification (35% on each finger)
- candidate lists of less than 5 people in 95% of cases
- candidate lists processed by expert matcher to give ‘yes/no’ result
- 5% false negative rate for the system (catches 19 out of 20 duplicate identity applications)
- 0.00006% false positive rate for an individual match (this is current typical accuracy)
- 500,000 matches per second (this assumes between 10 and 60 typical AFIS servers).

Combining all the techniques identified in this paper, we can calculate that the maximum population that could be supported by such a system would be around 27 million people. Such a system, however, would be at the edge of current accuracy and throughput achieved via conventional AFIS methods.

The Future of Large Scale Civilian Biometric Systems

As we have seen, the civilian requirement takes state of the art technology and pushes it to its current limits. Such leading edge technology is expensive and its implementation carries a risk premium. Such systems are therefore beyond the investment and skill reach of many nations.

However, Moore’s Law (which states that computer power doubles every 18 months) tells us that the price of this technology will reduce. Innovations such as new fuzzy searching technologies have already demonstrated their potential to revolutionise large scale biometric searching. In combination they provide scope for orders of magnitude improvements in accuracy, throughput and price/performance over the next few years.

Indeed, with two 25 million-plus person systems in production, enrolling their populations by 2004, it seems likely that the biometric industry will prove it can provide large scale civilian identity systems early in the next millennium. Once these projects are ‘tried and tested’, there is likely to be an increase in demand for the type of technology employed and a reduction in the risk of such projects.

Conclusion: The Global Consequences of these Systems

This demand will be lead in the areas of Asia Pacific and Latin America. In these regions, there are long traditions of using biometrics and specifically fingerprinting to identify their
national populations. The techniques outlined in this paper are an extension to their (often manual) existing systems in terms of reliability, accuracy and throughput. In the near future, large-scale civilian AFISs are also likely to prove more cost effective than these manual systems. It is highly likely, therefore that countries in those areas will see a great number of these systems installed.

By contrast, a great deal of reassurance and trust would need to be built up in Europe and North America before these systems could be widely deployed. It is possible, however, to define legislation and technology which provides identity integrity whilst preserving privacy and anonymity. Many good papers on this subject have been written and observing the recommendations and suggestions in these papers would help assuage people’s fears. Even so, it is unlikely that the US or an EU country will adopt a biometrically enabled identity system in the foreseeable future.

Eventual implementation, however, is highly likely. Whilst civilian identification systems at the moment are specifically focused on combating voter or welfare fraud, over time it is likely that their owning governments will perceive that providing secured, unique identities is a service to their overall economy. These trusted single identities could prove an enabling platform for improved government service delivery, and also perhaps, as the basis for electronic identities for Internet transactions and eventually e-business. Provided they could be implemented in a voluntary way and ensure the continued personal control over personal data then some form of secured personal identity will almost certainly be implemented in Europe and North America.

Hopefully, these civilian identification systems can be implemented sensitively and used wisely. If so, they may prove to be a positive force for privacy and a strong economic enabler in the next millennium.

**UNCITED REFERENCE**


**Notes and References**

2. Compaq, for example, now offer a fingerprint logon device as a standard option for their PCs.
3. The leading biometrics standards body is the BioAPI Consortium (which includes Microsoft, Novell, Compaq, IBM and others). They may be contacted at <http://www.bioapi.org>.
4. The definition of large scale identification here is for biometric systems capable of uniquely enrolling millions of people per year with an expected system size measured in tens of millions. The Iris recognition technology pioneered by Dr John G Daugman may also be suitable for this kind of system.
5. Even with a high degree of automation, experience has shown it is still highly advisable to train the clerks in taking fingerprints and photos correctly. Both large-scale AFIS implementations had some early difficulties in capturing good quality data. See Hopkins ‘A challenge to the biometrics industry’, op. cit.
6. It is worth noting at this point, that one of the large scale civilian AFIS systems which is enrolling, plans to implement over 75 servers to deal with its final throughput. See Ciriaco, op. cit. Large
amounts of hardware, memory and disk provide an expensive, but possible means of scaling throughput.
