BIOMETRICS
AND
LAW ENFORCEMENT

Clive Reedman

(Dedicated to my friend Jim Wayman who inspired me to write it)

INTRODUCTION

My aim in publishing this paper is to disseminate my own personal views as to the role that biometrics play at present in law enforcement. I also wish to present a view of how they may play a major part in the near and long-term future and what they offer to those involved in the Criminal Justice System (CJS). It is my contention that all of us involved in emerging technologies can always learn a lot from the past. Often we do not take the time to seek out the history of those technologies, in order to understand them and to learn the lessons that their origins teach us. Biometrics is no exception to this. How often do we hear about the incredible 'new' technologies that are shaping the future of human identification, when in reality our ability to use physical and behavioural traits in this way have been around as long as humans themselves? Our ability to accurately identify other people without employing technology 'external' to our own selves is phenomenal. Our own eyes are an incredibly efficient 'sensor' and our brains the most advanced matching and image storage devices that will ever exist. The 'comms' network that links the sensors, processors and image stores together does so with lightening speed and is able to outstrip the performance of any I.T. companies LANS, or WANS, even to the point of being able to self-repair damaged, or worn out parts automatically. I do not fully subscribe to Arthur C Clarke's view that "any sufficiently advanced technology is indistinguishable from magic." On the contrary, I believe that advanced biometric technologies are striving to become indistinguishable from our existing 'mundane' understanding of our world. A machine recognising a face in a crowd is not 'magic', but it does relieve our minds from a task that we do not always want, or need to perform.

I subscribe to a very simple definition of biometrics, namely, "the automated identification, or verification of identity through physiological, or behavioural traits." To me the most important word in the definition is 'automated'. It is automation that provides the greatest benefit of biometrics. Our human abilities outstrip the accuracy of biometric matching engines in almost all circumstances. As a fingerprint expert, I would challenge any algorithm developer, or salesman to prove that those algorithms could out perform a trained human being in the process of establishing a true match. It is the automation that provides the benefit. Even employing standard 'binning' methods I could perhaps search twenty reasonable quality scenes of crime (latent) marks a day against collections of rolled, inked impressions. Sooner, or later I will become tired, bored, or distracted. I will need to take a break and eventually sleep. My concentration will fail and I will make mistakes, but the processes my brain employs are closer to Clark's 'magic' than any machine will ever achieve. How often do we just 'know' that the person in the crowd is somebody we know, or have seen before, even after the shortest of glimpses, maybe at a considerable distance. What is it that makes us so sure? The answer is that our own brains are already able to achieve the 'holy-grail' of biometrics, namely 'recognition at a distance' (apologies to Jonathan Phillips). Without any effort, our data stores fuse the information that our 'sensors' collect, make comparisons and report results; the program written, updated and executed in our own portable super-computers. However, I cannot know everybody, or expect others to. Technology is a tool. Where it comes to identification, this tool provides many, many benefits, mainly benefits recognised through automation. As Vannevar Bush said in 1945, "The world has arrived at an age of cheap complex devices of great reliability, and something is bound to come of it."

In this paper I will seek to explain just why law enforcement relies so heavily on identification. I will put forward a proposition that it is only our modern ability to efficiently 'automate' identification techniques that has lead to the (re) emergence of biometrics and will complete it with my own view of how biometrics fit into the future of law enforcement.

WHY BIOMETRICS?

In fair and just legal systems there is no occasion when identification does not play a part in any crime investigation, or conviction. I cannot think of any circumstances where identification is not a vital element of investigation, or conviction. Investigation infers identification, be it the identification of propositions, theories, alibi's, or (most importantly), people. This fact raises the importance of identification in law enforcement above that of any other consideration. Everything else is ultimately secondary to the need to identify. Advanced communications systems, well-equipped and fast vehicles, helicopters and other such aids are the mark of a modern Police Service. The massive 'business' of maintaining an efficient law enforcement service has been made easier through computerisation and advances in management techniques and systems. Massive budgets are sought and spent each year. Initiatives come and go, as the system attempts to cope with a seemingly ever-increasing work rate. However, in the final analysis the whole CJS exists to fulfil two aims; the prevention and detection of crime. It is the second element of this mission that benefits most from the application of biometrics, but we must not lose sight of the fact that law enforcement itself requires an infrastructure bigger than most large companies support. This infrastructure includes a tremendous number of facilities, such as police stations, courts, prisons etc. It also increasingly includes the massive storage and processing of electronic information, often of a sensitive nature. The effective support of crime prevention and detection requires this infrastructure to be managed efficiently in terms of process, cost and security. A biometric product designed to secure entry to a Bank's trading room can equally be applied to the securing of a computer aided despatch room in a London Police Station. Encryption keys secured by a biometric and used to 'sign' electronic transactions between Solicitor's can also be applied to the signing of a police witness statement. The biometrics industry must not lose sight of this fact. Law enforcement is a major market, which has many of the same problems to

solve as any other institution, if not more. I do not intend to dwell on these 'business' requirements in this paper, as they are best dealt with in the normal commercial and security environments of the open market.

What is important is to seek solutions to the requirements of both the business processes that support the CJS infrastructure and the direct requirements of crime prevention and detection. Often there will be synergy between these two distinct areas in the application of biometrics, as these technologies have many applications that can cross the boundaries between business and direct law enforcement needs. A facial recognition system could protect a computer from unauthorised use, as well as providing a solution to finding a wanted person in a crowd of people. Fingerprints could provide the verification of a policeman's identity as he, or she books on and off of duty, or may provide the rapid identification of a suspect stopped in the street.

What biometrics offers the CJS now and in the future is the possibility of improving the overall 'clear-up' rate of crime, therefore increasing the confidence of the public in the system and their overall sense of security in society. Technology plays an increasingly important part in the direct fight against crime, but we must never lose sight of the fact that public confidence in the system involves a desire to see the human face of policing. A highly effective and accurate town centre CCTV surveillance system using facial recognition may actually prevent more crime than any number of uniformed police officers 'walking the beat', but public feelings of security may better be served by a uniform, rather than a camera. Clearly a trade-off may be required and overall strategies established, or refined to solve the fundamental problem of operational efficiency versus public perception.

The need to identify, or verify identity has been understood within the CJS for many years. The recording and searching of physical characteristics in support of law enforcement is nothing new. Indeed, it can be argued that the whole science of 'biometrics' has been used within the CJS for over a hundred years. The next section of this paper explores this history and seeks to raise the dangers that need to be considered as we move forward into an increasingly automated biometrics future.

A NEW SCIENCE?

In 1879 a twenty sixteen year old man joined the Paris Police as a Clerk and was bored almost immediately. However, the impact that this man would have on the science of human identification and the modern biometrics industry is almost inestimable.

Alphonse Bertillon was the son of an anthropologist who had spent a large part of his career attempting to prove the theory that no two human beings possessed identical physical characteristics and that these differences were measurable. Alphonse soon found a way of improving his rather dull job by convincing the Paris Police that he should be allowed to experiment on prisoners in order to devise an effective means of identification. The motive of the French authorities in allowing Bertillon to proceed is not as clear as it would first seem. French law at that time presumed guilt. It was for the accused to prove innocence. Just how important it was for the authorities to have to prove that they may have dealt with an arrestee before, I do not know, but certainly the presence of a past criminal history must have added to any sentences metered out. However, Bertillon was given permission and despite a deal of initial scepticism he employed his father's measurement techniques successfully for three years, 'positively' identifying hundreds of prisoners. His fame rose and in 1892 he became the first Director of the Paris Bureau of Identification and was eventually awarded the Chevalier Legion of Honour for his work.

The Bertillon 'amphropometric' system of measurement spread throughout Europe and quickly crossed the Atlantic to North and South America. It was not biometrics in the true sense, but the general aim of identification through physiological traits was the same. Bertillon devised a measuring and recording routine that required many separate measurements to be taken, starting with a sub-division based on the size of the cranium. The body would be further measured and sub-divided in more and more detail and the details recorded. Bertillon's 'eleven measurement' system was adapted, improved and added to as the techniques were adopted by other agencies, until over one hundred separate measurements could have been taken.

Obviously, it is not possible to transpose the early science of 'bertillonage' with the modern science of biometrics. Certainly, the aims of measuring and being able to search physical characteristics are the same, but there is one major element missing; that of automation. The system was time consuming, both in the recording of the characteristics and in the comparison. A full examination could take more than an hour per prisoner to perform. However, some of the ideas and principles of the system are clearly still with us today.

Confidence in the Bertillon system didn't last long. A lack of care and inexperience amongst those taking measurements was soon being blamed for a number of 'mistakes'. These errors and the fear in Britain that incorrect sentences were being given, or even served lead in 1898 to the establishment of a Royal Commission, charged with adjudicating on the best method of establishing identity. The Commission sided with Sir Francis Galton who argued that the statistical interpretation used by Bertillon was flawed. Galton, in his 'Memories of my Life' wrote:

> *There was...a want of fulness in the published accounts of it, while the principle upon which extraordinary large statistical claims to its quasi-certainty had been founded were manifestly incorrect, so further information was desirable. The incorrectness lay in treating the measures of different dimensions of the same person as if they were independent variables, which they are not. For example, a tall man is much more likely to have a long arm, foot, or finger, than a short one. The chances against mistake have been overrated enormously owing to this error; still, the system was most ingenious and very interesting.*

Galton won the day and the Commission concluded that in Britain the Bertillon system should be replaced by a more reliable means of identification. This decision lead directly to the establishment in 1901 of the Fingerprint Branch at New Scotland Yard under the leadership of Sir Edward Henry, now best known for his still widely used fingerprint classification methodology.

Despite the decision of the British Royal Commission and indeed the existence of an even older national fingerprint system, established under Juan Vucetich in La Plata, Argentina in 1896, the Bertillon system continued to be used and trusted. However, a further and terminal 'nail in the coffin' was to come. This was the now famous case of the 'Will Wests'.

In 1903 a prisoner arrived at Leavenworth Prison, Kansas and was subjected to the normal methods of reception, including the taking of his physiological measurements required by the Bertillon system. Will West's index card was written and he was introduced to his new 'home'. All seemed normal, but a clerk at the prison who had taken the measurements was sure that he had seen this man before. A search of the records indeed revealed a record for Will West, who did have almost exactly the same Bertillon measurements as the new intake. However, there was a problem. This Will West had been incarcerated two years earlier in Leavenworth and was STILL there. Re-measurement of the unrelated men confirmed that their measurements were almost identical. Bertillonage could not have told them apart, but one thing did differ; their fingerprints! The final nail had been driven into the coffin.

There is apparently now some doubt being raised as to the Will West incident, with speculation that they had indeed been twins. However, the fact remains that the Bertillon system could not have divided them adequately to prove beyond doubt that they were different people. Fingerprints could do this and for the past one hundred years they have become the mainstay of person to person identification around the world. But identification in law enforcement consists of more than person to person identification. The next section explores these three types of identification.

IDENTIFICATION IN LAW ENFORCEMENT

Law enforcement employs three distinct, but not inseparable types of identification in the prevention and detection of crime. I class these as, person to person, latent to suspect and biometric 'image' to suspect. Let me take each of these in turn:

Person to person identification

In the vast majority (if not all) of countries throughout the world there is now only one principle method employed for the 'measurement' of a person to establish whether that person is known to the authorities, or is who he is suspected of being. That method is of course, fingerprints. The taking of a set of 'ink on paper' and now increasingly 'livescan' prints from arrested persons is normal. These fingerprints are routinely used to establish one of four things, namely;

1) that a person is known,
2) that a person is not known,
3) that a person is known and is who he is suspected of being,
4) that a person is known, but is not who he was suspected of being.

It is fingerprints that link that person to his criminal history and increasingly this process is being automated through the use of Automated Fingerprint Identification Systems (AFIS). Many countries throughout the world have adopted this well understood and stable biometric technology. The speed and accuracy of a modern AFIS system is astounding, with millions of sets of fingerprints being searched in minutes.

> *Care must be taken to understand that the technology behind and the requirements of a large-scale AFIS system are very different from those of a small scale, far cheaper 'civilian' biometric fingerprint system. AFIS systems are capable of conducting high volume one to many searches against very large databases. They typically achieve these using minutiae files extracted from ten fully rolled fingerprint impressions, captured at a high image resolution. Civil application biometric systems are typically designed for one to one verification and utilise single finger capture of an image much smaller and of lesser quality than that needed by an AFIS system.*

Governments have invested large amounts of money in AFIS and it is unlikely that their predominance as the principle person to person identification method will be challenged in the near future. However, the emergence of the new biometric technologies and their increasing accuracy and falling costs, could challenge this supremacy in the longer term. Is it unreasonable to start considering now the taking of an iris pattern from an arrestee? Certainly, the 'maths' behind iris recognition technology seems convincing when compared with fingerprints. It is possible now to conduct high penetration searches using iris recognition technology, so why are we not clamouring to start immediately on the road to replace fingerprints for person to person identification? There are a number of reasons, including the protection of existing investment and the risks surrounding single supplier sources. It is also possible that legal recognition will not be easily obtained. It has to be remembered that even now in the UK, fingerprints are not recognised as totally infallible, rather as 'practically infallible'. The legal recognition that statistically, a persons fingerprint may not always be different from another persons, but that the chances of both of those people ever being in the same 'experience sphere' are so slim to be almost impossible, took 52 years to achieve in the UK. Expert evidence may only be given in court by a registered fingerprint expert, who will have spent at least five years in the field and will have passed a number of examinations of his/her competency.

How long would it take other biometric technologies to even reach the level of 'practical infallibility' and how do we establish the expert base required? All of these questions need to be answered before any country moves away from the tried and trusted use of fingerprints for person to person identification. What would be the real drivers to make such a radical move? Perhaps we need to seriously consider not only the potential gains in accuracy, but also the true benefits of that increase in accuracy. Maybe, even now with the advanced AFIS systems readily available, we do not need to have a human being in the 'loop' at all. Do we trust the accuracy enough to permit a machine to make the final decision? Are AFIS systems accurate enough to pass the final decision to a non-expert, such as a Police Officer, who could utilise other information like scars, tattoos and photographs? Perhaps we can consider the 'layering' of biometric identification techniques to improve the certainty level even further. Why not consider combinations of fingerprint, iris, face and voice, maybe even DNA? Cost and process efficiencies may be obtainable by removing the human from the loop, in addition to increased accuracy, but there is a long way to go yet.

Latent to suspect identification

The golden rule of crime scene investigation is that 'every contact leaves a trace'. In fact this often quoted rule is a paraphrasing of 'Locards Law', i.e. when two objects come into contact, there is an exchange of material from each to the other'. There are no exceptions to this rule; every contact does indeed leave a trace, however small it may be. Crime scene examination is very much about finding these 'contamination traces' between objects, be they between human beings, human beings and objects, or between object and object. If I shake hands with a friend we will exchange skin particles, amino and fatty acids, salt and other contaminants that may be present, such as hand cream, oil etc. Where a 'contact trace' is relevant in the investigation of a crime, it is the job of the crime scene examiner to realise the potential evidential value of such exchanges. The evidence must be collected, preserved and further contamination prevented until the forensic scientist can examine it. The list of commonly collected trace evidence is an ever expanding one, as tools for its' collection and analysis become more and more sensitive and advanced. Classic evidence includes DNA samples from blood, semen, or hair; fibres from garments, shoe and tool marks, glass fragments, wood splinters, paint flakes and of course 'latent' finger, or palm marks. In fact an almost endless number of possibilities exist.

Crime scene evidence has two uses in law enforcement, namely; providing the evidence that links a suspect with a crime and providing a suspect, or list of suspects who may have committed the crime. Obviously, in the first instance it is necessary to have some suspicion as to the possible identity of a perpetrator. For example, a victim may have accused a man of rape and the contact evidence examination would concentrate on exchanges of material between the victim and suspect and possible the suspect and the crime scene. Blood typing and DNA analysis would be principal in such an examination, but other trace evidence would be relevant, depending on the circumstances. If a suspect exists and the aim is to try and place that suspect in a position whereby he could have committed the crime, access needs to be gained to the evidential material that would provide that evidence, such as clothing, or the suspect himself.

The use of trace evidence to provide the suspect(s) where none already exists is more complex. Should the rape victim not have known her attacker, the material exchanged can only be collected from the victim, or crime scene. The problem then becomes one of using that evidence to 'narrow down' what may be an immense list of possible suspects into one manageable within the crime investigation. Maybe semen traces provide a blood type, or a fibre found on the victims clothing could be found to be of a rare material. In other words, the two circumstances resemble a one to one match in the first instance and a one to many search in the second.

So where do the biometric technologies play a part in the process analysing and applying trace, or 'contact' evidence? In either a one to one, or a one to many comparison it is of course necessary to have a 'sample' against which the comparison can be made. At some point in the process the suspect, or potential suspect must have provided a 'respondent' sample to compare against the 'enquiry' sample relevant to the crime. Clearly, a high proportion of such enquiry samples will not represent physical characteristics of the suspect, e.g. a fibre from clothing worn by him. However, some actual biometric samples could exist for a number of reasons. The classic example is of course fingerprints. Maybe the suspect (known, or unknown) has a criminal record and latent fingermarks have been found at the scene of the crime, or on articles related to it. In the UK, the identification of such marks has been the main job of Police Force Fingerprint Bureaux since they were established and the science is a well understood one. Latent crime scene mark identification has benefited tremendously over the last fifteen to twenty years by the advances in AFIS technology and improvements to system efficiency and accuracy continue to be made on a regular basis. But what other biometric samples may be available to assist in the solving of crimes containing 'physical' trace evidence? At present there are very few, but as the possibilities of biometric technologies increase the list may become larger. Maybe DNA profiles could soon become as commonplace for use as access control templates, as hand geometry templates are now. Perhaps the advances in extracting such DNA profiles will make it possible to enroll into a biometric system by simply collecting a minute sample of sweat from a finger.

Even if the number of biometric systems that use physiological samples, which may also be found as trace evidence at crime scenes increases, there is one major problem for law enforcement. Fingerprints are a physiological sample, but the fact that we can match them with 'accidentally' donated crime scene marks (developed bodily fluids) relies on the fact that the 'enrolment' set was taken in line with a legal precedent. The use of biometrics in civil applications requires that an element of trust exist in the system. Already some governments require the collection of fingerprints from all of their citizens. Maybe soon this will expand into the DNA arena. Would a government planning to introduce national identity cards, secured by a biometric, prefer to use an iris pattern template against a DNA template, when a national database of DNA templates could offer the chance to match physical trace evidence and an iris pattern database couldn't? DNA as a 'mainstream' biometric will, I am sure, become a reality in the not too distant future and how long will it be before ten AFIS standard fingerprint templates are taken, even for 'civilian' applications? Access to such data by the law enforcement arm of governments could provide them with a great opportunity to solve more crime, but there are obviously a number of civil liberty and privacy issues surrounding such a possibility.

Biometric 'image' to suspect identification

The first two areas of identification that I have discussed above are not new. Emerging biometrics do effect them both, but the general processes of 'person to person' and 'latent to suspect' identification are tried and trusted over many years. Advances are being made in both areas and biometrics could lend a great deal towards this advancement. However, there is one area of identification in the law enforcement arena that stands to benefit from the emergence and improvement of biometric technologies in a more immediate and dramatic way. Explain face recognition to a police officer and without prompting a whole range of potential uses will be offered up. How often have I been told about the difficulties involved in searching hours and hours of CCTV footage for a single individual, or heard about the almost impossible task of trying to match a poor quality facial image on a Bank's video tape with an unidentified armed robber. What about the known terrorist who may be trying to gain access to a political parties conference? Maybe after explaining voice recognition the same officer may offer up examples of audio recordings of kidnappers, never identified. All of these possibilities represent a scenario where there may be no 'physical' trace evidence, or any idea who the individual may be at all. Manually attempting to find a 'face in the crowd', or identify a suspect from pictures of known offenders is a notoriously difficult task, as well as a very costly one in terms of police time. Just watch a single video monitor in a local council's control room for hours on end waiting for a particular individual to appear for a second or two and you will soon realise the concept of 'face blindness'. See the success of a television programme such as the BBC's Crimewatch, which relies heavily on the fact that images can be shared amongst a national audience and you will soon grasp that the chances of identifying an individual increase dramatically the wider that audience is.

In no other form does my contention that identification is the most important part of any police investigation become more relevant, than where the only evidence is such a biometric 'image'.

However, there are a number of obstacles that have to be overcome before the effective and efficient identification of such biometric images becomes a reality. Firstly, we have to consider the state of the biometric technologies themselves at this current point in time and the chances of them improving in the foreseeable future. Face in the crowd and automated witness album searching are with us now, but just how effective and accurate are they? Is the success of a CCTV/Facial Recognition implementation in London's East End a success because it identifies quickly and accurately the faces of known offenders? Or is it successful because of its deterrent factor? Does such a system merely displace crime away from the 'protected' areas and possibly even make the situation worse by altering, to a more violent type, the crime that is committed by those very individuals? Is it feasible that facial recognition will one day soon become accurate enough for the police in Nortumberland in the North of England to expect to 'hit' against a known offender from London, whose facial template may be held as part of a national collection? What issues are there to consider regarding arrest 'mugshot' images in terms of national capture standards, image compression, the particular facial recognition technology applied, etc? How would a national facial image database be used and what is the true business case behind it? What legal and civil liberty implications are there to consider and are changes in the law necessary to make it a workable proposition? All of these and many more questions need to be answered before any further move is made towards the establishment, or expansion of such law enforcement based databases and systems.

My personal view is that the identification of biometric 'images' is of such importance in law enforcement that all efforts need to be made now to put in place the 'building blocks' of efficient, accurate and cost-effective solutions. However, I also firmly believe that all of the civil liberty and privacy issues need to be addressed in parallel and debated fully amongst a wide audience. Perhaps the routine collection of facial images from arrests is commonplace now and the expansion of small local databases into nationally held collections is a major step towards preventing and solving more crime, but the public need to understand just why it is necessary and desirable. As a tool to assist with witness album searches, i.e. an unknown face against many known faces, a national database is easy to 'sell' to the public. However, as a database against which facial images of the general public would be routinely compared against known offenders to find the 'face in the crowd'?

CONCLUSION

Biometrics offers many advantages to the law enforcement community. These advantages fall into two distinct areas, but are not mutually exclusive. Firstly, the business, process, cost and security advantages that biometrics bring to any organisation can be applied throughout the CJS, which is a collection of agencies, all of which have premises and data to protect. Secondly, there are the direct advantages to law enforcement itself as applied to the two major objectives of the prevention and detection of crime.

Identification always plays a part in crime investigation and conviction in a fair and just system. Clearly, there is a wealth of experience and expertise already applied in these fields and technology is enhancing them at a rapid pace. However, biometrics opens up new possibilities and challenges, which may increase dramatically the effectiveness of the law enforcement community.

The possibilities cannot all be mentioned in this paper, because of space and the fact that many more ideas exist than I have even begun to think about. I hope that this short paper will stimulate debate and bring even more of these possibilities to the fore. My real hope is that biometrics does not go the same way as Bertillonage and that history does manage to teach us the lessons to be learned from one hundred years ago.

Clive Reedman

Creedman@btinternet.com