Computerised Facial Recognition Systems: The Surrounding Legal Problems

Michael Bromby

9906435

LL.M Dissertation

Faculty of Law

University of Edinburgh

September 2000

Abstract

Computerised facial recognition systems have developed to the extent that they can compete with and aid human experts with cases of disputed identity. With the advent of CCTV, facial recognition has now become a tool for crime prevention and detection. As the use of such systems becomes more widespread, the legal system is now having to deal with the contentious issues surrounding the implementation of new and developing technologies.

> *"The central problem in face identification is how we build stable representations from exemplars that vary, both rigidly and non-rigidly, from instant to instant and from encounter to encounter."*[1]

Biometric analysis is based on measurable characteristics of the face, which may be used to recognise or identify an individual. Many technologies have been developed for person recognition and identity verification based on information from fingerprints, face analysis, voice, retina and iris recognition.

[1] Bruce, 1994

Scope of Analysis

Due to the vast nature of such a developing technology, this report will introduce facial recognition through proposed psychological models for human facial recognition and show how this has been incorporated into computerised recognition systems. An exposition of case studies involving facial recognition will give some evaluation as to the legal usage of computerised recognition before the reliability of such systems is assessed. The potential for miscarriage of justice will then be examined using anecdotal evidence and legal cases to demonstrate how such problems have evolved by using recognition technology.

As this study into computerised facial recognition systems draws on research from a variety of disciplines such as psychology, computing science, artificial intelligence, sociology and law the subject will be introduced and discussed to provide the reader with sufficient understanding of these disciplines to be able to recognise the legal problems surrounding computerised facial recognition.

Table of Contents

Chapter 1

Introduction

This chapter aims to introduce the theme of surveillance, relate public and private interests to CCTV and outline some of the legal history surrounding facial identification.

A History of Surveillance

The etymology of the word 'surveillance' arises from the French language, meaning 'to watch over'. There are many techniques that may fall into the broad category of surveillance, some of which will be discussed in this chapter. The aspect of facial recognition will be the main theme of this paper, concentrating on legal problems associated with computerised recognition in both public and private spheres. For computer systems to be able to identify and subsequently recognise subjects, suitable surveillance capabilities must also be present; the immediate issues surrounding such invasive techniques will not be dealt with here as they must be *in situ* in order that the facial biometric systems may function.

Surveillance is not a modern concept: records have been kept containing details of people's whereabouts, possessions and wealth over centuries. The ancient Egyptians maintained population records for improving control over tax, military operations and immigration; the Book of Numbers describes the great census of the Israelites; and the Doomsday Book of 1086 can be seen as the precursor to today's Census prepared every decade by the governmental records office.

These ancient records were prepared laboriously, taking many years to assemble, from which only a limited number of simple facts could be deduced such as population size, density, birth rate etc. These statistics were often out of date by the time all the data was collated. With the advent of printing, the so-called Gutenberg

revolution[2], administrative power could be increased and beaurocracy was firmly established. Extensive records could not only be maintained, but also distributed efficiently in vast numbers to various individuals, institutions or amongst nations. With modern computerised technology and digital storage even greater possibilities arise: storage capacity is almost unlimited, file copying and transfer occurs instantaneously, trends may be observed and hypotheses calculated to provide immediate predictions and results.

Surveillance, therefore, exists in modern society. The way it is used and the ways in which it is, or should be controlled may differ according to the goals of the user. The following sections briefly examine public and private sector interests in surveillance.

Private Sector Interests

Businesses, enterprises and companies regard personal details as valuable commodities. They can be used to increase their market and target individual sales; such details may be bought and sold to other parties, also for a price. Surveillance of customer consumer habits demonstrates the Marxist theory of information capitalism[3] which customers endure for their loyalty card rewards and special offers tailored to their individual tastes.

Foulcault's theory of power[4] is exemplified when surveillance occurs in the workplace. Although there may be a capitalist drive to improve the efficiency of the staff by observing them, it is the knowledge that the staff are being observed that drives them to meet targets or observe certain work-place rules. A certain level of observation may be reached before the act of surveillance encroaches on the employees' privacy and becomes a threatening or critical eye undermining their ability to work productively and harmoniously.

[2] Lyon, 1994. Pg. 23
[3] Lyon & Zureik, 1996. Pg. 6
[4] Lyon & Zureik, 1996. Pg. 7

Public Sector Interests

As servants of the State, democratic governments assume the right to monitor their citizens to ensure that fairness and equality prevails. Access to services, the law and justice are seen as justifiable reasons to implement suitable levels of surveillance in a rational approach to providing a solution to specific problems. The Weberian approach[5] argues that new technology is not the cause of new surveillance practices, but that such techniques can aid the functioning of the state institutions, which in this case is the prevention of crime and disorder.

Foulcault's theory of power again extends to the public sector with the benevolent desire to protect society and to punish deviant behaviour. As seen by the Bentham's Panopticon[6], the desire to become deviant is repressed by the knowledge of close observation. Therefore the positioning of CCTV cameras (as a substitute for a police officer) may serve as tools of crime prevention, more so than as a form of crime detection. Examples of such control are popular themes for twentieth century literature such as Orwell's classic 1984[7] and Brave New World by Huxley[8] whereby society is ubiquitously controlled to prevent the smaller outbreaks of disorder that are evident in today's society.

Computerised Recognition

The many forms of computerised human recognition have traditionally been positive acts of recognition, with the individual actually wanting to be identified by the machine. It has often been performed by one of two measures: what you know (such as a password), or what you have (such as an identity card) to allow entry into the computers records and databanks. These two forms of security are often compromised if someone comes into possession of a stolen or fake ID card, or learns the current password, making the system vulnerable to unauthorised access. To make the system more secure, the 'protectors' must be aware of the technologies and capabilities of the criminals or hackers who wish to break into their system; with

[5] Lyon & Zureik, 1996. Pg. 7
[6] Lyon, 1991.
[7] Orwell, 1954.
[8] Huxley, 1955

many security systems being broken soon after their implementation, organisations are constantly looking for ways to further improve their security.

A third category of secure identification has evolved that may be labelled as *who* you are, which is less easy to mimic. Biometric identifiers such as your fingerprint and other unique personal features are being exploited by commercially available technologies currently being used in many environments to determine a person's identity. Such methods of identification may not necessarily involve positive participation by the individual the computer seeks to recognise, thus allowing the system to detect intruders or those who may wish to conceal their identity.

The patterns of the iris, like the contours of our fingerprints, are unique among individuals and can be used as a basis for biometric recognition. Two new commercial developments involving iris recognition are of particular interest. Firstly the UK Building Society, Nationwide, is pioneering an iris recognition scheme in place of the traditional Personal Identification Number (PIN).[9] The camera can locate the iris and measure some 266 characteristics, which is then translated into a unique code for that individual. The code is carried within the magnetic strip of the bank cash-card, and can be compared to the user of the automatic cash dispenser to verify customer identity. Unlike the PIN, this code cannot be discovered by anyone else, or forgotten by the true user.

The second use of iris recognition was reported in the US Government Computer News in September 1999.[10] The US armed forces have taken an interest in biometric recognition as a replacement to passwords for access to computers and biological weapon controls. Traditional passwords were becoming increasingly difficult to remember, as multiple eight digit codes were required for various systems. This security system had advantages over alternative methods: as voice recognition fails through protective headgear, and finger/hand prints cannot feasibly be performed with rubber gloves. Iris recognition was favoured as a facial biometric analysis, even functioning correctly through plastic shields and protective glasses.

[9] As Reported in *The Guardian*, Tuesday 14 March 2000
[10] Daukantas, 1999

Iris recognition, however, appears to be useful only when the subject is close to the scanning device and allows a scan to be performed voluntarily. Alternatively, it may be used when a suspect is apprehended and forced into an iris scan in a similar manner to the recording of fingerprints in police custody. The fingerprint method, however, has a distinct advantage over iris recognition. 'Trails' are left by the individual that can prove where the individual has been and what they have touched. The prints may be lifted after the suspect has left the scene, whereas with iris recognition the only available trails are from CCTV cameras that would not provide the desired resolution to scan the inner part of the eye. Human identification and recognition from a distance must employ a more general form of recognition to allow law enforcement agencies to exploit the use of computer technology.

Taking advantage of the CCTV cameras, the use of crime scene pictures to identify criminals was becoming commonplace. Previously only the eyewitness could provide evidence to link a suspect to a crime scene, with the advent of CCTV, the judge and jury could see for themselves how similar the accused and the assailant's images were. However, the clarity or CCTV images and the tendency for security videos to photograph images one or two seconds apart gave poor grounds for accurate recognition. The lighting levels and face angles could also hinder human recognition pathways.[11] By taking measurements of the face and analysing the face as a whole, a further biometric identification process was established, allowing computer systems to make their own assessment of similarity between the accused and the assailant. These systems became important when CCTV footage was too poor for human recognition and where no reliable eyewitnesses were present.

As with any new technology, the use and reliability of these methods, particularly when they form the sole piece of evidence for a prosecution case, are of interest to the legislature, judiciary and citizens alike.

[11] Studies by Hill and Bruce showed diference in lighting and novel face angles to be a major distractor for positive identification. Hill & Bruce, 1993

Landmarks in the Juridical System of Facial Identification

The first instance of a photograph being admitted as evidence in a court of law was in 1864.[12] In 1892, an artist's impression was presented as evidence[13] and subsequently with the advent of PhotoFit, Identikit and the computerised E-Fit and CD-Fit packages, images constructed from witness descriptions became common-place in many criminal cases of theft, assault and kidnapping.

With CCTV becoming popular in the 1980s, actual photographs rather than a likeness of the accused became available to support the case put forward by the Crown Prosecution Service. With a number of Expert Witnesses providing their opinion in cases where identification was an issue, some notable judgements in the Court of Appeal were of significance to the admissibility of expert evidence concerning identification through facial mapping and biometric analysis.

In 1993, it was held that where identification was an issue, "there was no reason why expert evidence should not be given, if it could provide the jury with information and assistance."[14] By 1994, facial mapping through video superimposition had become real evidence, to which no special rules applied. A comparison was made to fingerprint analysis, which may require an expert witness to assist in the interpretation when the evidence is not sufficiently intelligible to the jury without any help.[15]

The Kerrigan case brought attention to the interpretation of such expert evidence. The judge, on summing up to the jury stated:

> "Mr. Oxlee [the imagery expert] is strongly criticised by Mr. Magarian on behalf on the defence saying that this is really just a subjective assessment, it is not scientific, he is just a man with a magnifying glass. There are no measurements or calculations or anything of that kind. You

[12] R v. Tolson (1864) and R v. Hindson and Ashby (1896).
[13] Mille v. Lamson
[14] R v. Stockwell, Court of Appeal, March 4-8 1993
[15] R v Clark, Court of Appeal, October 9 1994

> must consider those criticisms made by the defence as well as the submissions made by the prosecution."[16]

The Appeal Court deemed the use of such evidence as acceptable by both the prosecution and the defence, when similarities and differences could be identified from video images, as acceptable.

As the developments in facial identification advanced, more cases have employed expert witnesses to analyse CCTV footage and custody photographs when identification is an issue. Biometric analysis and facial recognition will be discussed in the following chapter, with particular attention to automatic recognition and how it compares to human recognition.

[16] R v Kerrigan, Court of Appeal, June 11 1998

Chapter 2

Human Recognition

To be able to assess the potential for computerised facial recognition, the capabilities of human recognition must be analysed to demonstrate whether biometric identification is more or less successful than human recognition.

Familiar and Un-familiar Faces

Psychological experimentation into facial recognition can be divided into two general areas: the recognition of previously unfamiliar faces, and the processes associated with the recognition of familiar faces. From extensive research[17], it has been shown that subjects perform well at recognising familiar faces and generally perform poorly with previously unfamiliar faces. Evidence has shown that within the brain, two distinct pathways to recognition are evident through studies into familiar and previously unfamiliar recognition.[18] As previously unfamiliar recognition is important for forensic identification, techniques have been put forward to improve the success rates of previously unfamiliar recognition. However, the results have shown the 'training' of individuals has not been particularly beneficial, exhibiting marginally worse error ratings. If successful, recognising previously unfamiliar faces is one of several areas where automatic facial recognition through a computer may perform better than its human counterpart.

Despite the general success of human identification, studies by Young[19] identified an alarming frequency of mistaken identity in everyday situations by the average population. Four major types of mis-identification were highlighted:

1 - A familiar person went unrecognised

[17] Bruce & Young, 1986.
[18] Studies by Ellis et al., 1979; Klatzky & Forrest, 1984; Faw, 1992; Valentine & Bruce, 1986

2 - An unfamiliar person was mistakenly or incorrectly identified

3 - A seemingly familiar person was recognised, but could not be identified

4 - Only partial details of a familiar person could be retrieved from memory

This is of particular concern when CCTV footage is of poor quality and the chance of mis-identification is increased, as most CCTV targets are unfamiliar to police officers and the subjects of attacks. Identification parades have been criticised as to their reliability as evidence, however the jury continually regard such identification quite highly, obviously estimating human recognition to be considerably accurate. The errors, and success rates, in human recognition can be quantified to assess how good individuals are at memory recall and facial matching. This can be directly compared with computerised recognition success rates. Even if automated systems perform marginally poorer, they may still be of some value for law enforcement agencies as computers can work reliably around the clock and provide a constant level of quality in their output. Human recognition levels may vary from individual to individual and can be depreciated by other external factors such as mood, stress, brain activity levels and may feel under pressure when their testimony is brought to trial.

From a landmark case in identification, the following comments were made in the House of Commons:

> "The case against Mr. Virag rested on identification evidence. On the face of it, this was substantial - he was picked out on properly conducted identity parades by no fewer than eight witnesses: three officers of the Gloucestershire police, two officers of the Liverpool police and three civilian witnesses. However, a number of witnesses did not identify him, and those who did were mistaken."

Secretary of State for Home Department 08/04/74 [20]

---

[19] Young et al., 1985.
[20] Hansard 1974 Vol. 872 Pg. 46

A comparison of two computer-based recognition systems with human recognition was carried out[21] in a study involving a graph matching system and a principal component analysis system. The two systems had a remarkable similarity to the human recognition pathways suggested for familiar and previously unfamiliar faces.

Principal Component Analysis (PCA)

This facial recognition system[22] relies on analysis of the image as a whole and is poor at recognising faces under different luminosity or those with different hairstyles as demonstrated by the examples in figures 1 and 2. Pixel colour and colour distribution is analysed in a similar way to the way in which the composition of a 'painting by numbers' picture may be described. The numbers refer to a given colour and the areas of the painting represent the distribution of the colours. With facial images the hairstyle dominates a large area of the image and the difference in pixel colour contributes greatly to the 'Eigenface' that is constructed as a reference for future comparisons. Every human face can be compared to each of the 150 existing reference 'Eigenfaces' within the PCA system and a degree of likeness assigned to each one. Only the 40 highest Eigenfaces are required to reconstruct a 99% accurate composite face of the initial subject due to the limited number of differences between every existing and possible face.[23]

[21] Hancock et al., 1998
[22] Pentland et al., 1993
[23] Turk & Pentland, 1991

Figure 1. A composite face artificially constructed using computer software.[24]

Figure 2. The basic facial features from figure 1 with different hair and shoulders superimposed.

At first glance, the two images appear to be a different person. Closer examination by looking at the inner facial features reveals that the images are of the same person.

As these faces are previously unknown, the brain recognises the features associated with the face such as short dark hair, rather than the actual face details such as eye

[24] Both figures are composite faces composed using the identikit software PROfit as downloaded from www.zeda-abm.com

shape and the positioning of the nose and mouth. The computer, likewise, recognises the shading and area coverage of the hair and other features, although it may make calculations that are more accurate than human recognition.

The faults with such a system occur when changes in luminosity affect the shading of the face; the angle of the head reveals different areas of the face; expression changes the position of the eyebrows and the mouth. Human identification and recognition pathways may be able to take these factors into account through interpolation. Quite often the human mind can imagine how a previously unfamiliar face may look when a surprised expression is maintained or vice versa. However, differences in the hair length and facial features occur on a daily basis resulting in drastic differences over weeks, months and years that can cause failures in the recognition systems of both humans and computers.

PCA can be a useful tool for detecting the gender, race[25] and age of a target using the location and size of the facial features as a general guide for categorisation. However, a standardised picture is still required unless some other system could interpret the head rotation and take into account the lighting levels and the distance between the subject and the camera. Although this would not lead to identification, some form or recognition is still being performed by the Principal Component Analysis.

It is suggested that first-glance identification and recognition of previously unknown faces in human recognition follow a similar pathway to the PCA methodology. As the counterpart human recognition pathway is considered to be significantly poorer than familiar recognition, it may seem logical to suppose that PCA recognition will perform poorer than the following graph matching system.

Graph Matching

This system of computerised facial recognition[26] concentrates on examining the inner features of the face, and is able to recognise the same person even when half of the

[25] Zhao et al., 1997
[26] Wiskott et al., 1995

picture, such as the hairstyle, is removed. Measurements of the location and distance between facial features are taken to provide a point of reference for further comparisons. This analysis of biometric target points located around the eyes, nose, mouth etc. is the suggested model for human recognition of familiar faces as changes in the hairstyles and clothing of the people who we are familiar with do not prevent us from recognising them. However, a computer system can be directed to analyse only the area around the eyes and the nose, whereas human vision cannot be so selective for unfamiliar recognition. The surrounding facial shape and attributes will always be recognised by humans and will become involved in the decision process as to whether the subject is familiar, leading to the subsequent retrieval of semantic information such as their name and profession etc.

Graph matching succeeds on many of the failure points identified by the PCA method. The angle of the head can be taken into account using algorithms; hairstyle and daily changes in luminosity do not affect the positioning of the facial features; and expression has a less profound effect on the algorithm than observed with PCA.

With graph matching, the genotypic features are being used for biometric comparison. These qualities change only slightly over the subjects' lifespan compared to the daily changes observed in the analysis of phenotypic features used in PCA. The performance limitation of genotypic analysis is the false identification rate, for which Daugman[27] uses the birth rate of monozygotic twins. This leads to a minimum false acceptance rate of approx. 0.82% due to birth rate alone.[28] Phenotypic analysis is limited by the false reject rate and is a reflection of environmental contributions to a person's appearance that is less easy to quantify.

The similarities between the computerised recognition systems and the proposed models for human recognition are encouraging for the development and success of further advanced recognition programs. It is not entirely proven how familiar recognition is performed in humans, however, graph matching reveals a similar

[27] Daugman, 1997

[28] A secondary calibration is provided by the extent of the gene pool. Full siblings, double cousins and a given parent and offspring can provide equally similar facial features. Such an example is Robert F. Kennedy and his son Michael in adulthood.

performance for computerised recognition compared to the human error and success rates.

It may be that familiar recognition works by the storage of multiple viewpoint images of the person and performing multiple analyses using PCA, graph matching, and other techniques not yet elucidated.[29] Multiple techniques will be discussed in a later chapter as future developments for computerised facial recognition systems.

[29] Interview with Prof. V. Bruce

Chapter 3

Computer Recognition

This chapter aims to examine some of the technological adaptations of biometric identification that are more appropriate to crime detection and prevention.

Facial Recognition Systems

Recently, the Defense Advanced Research Projects Agency (DARPA) has canvassed for potential computerised recognition systems capable of accurately and reliably identifying both known and unknown subjects from a distance.[30] The aim of the project is to promote the development of facial recognition systems, providing a forum for academic, public and private research with the aim of increasing the use and improving the reliability of such systems. The following sections will look at some computerised facial recognition systems that concentrate on the facial features and calculate their relative positions on the face from a CCTV or similar camera placed at a limited distance from the subject.

Current Applications

As discussed in the previous chapter, the biometrics of the entire face have established themselves as a capable means of identification. The positioning of the facial features within the face is just as unique amongst individuals as their DNA, iris pattern or fingerprints. Many software companies and solution specialists have developed software that employs computerised facial recognition to varying extents.

The commercially available product FaceIt® was developed by Visionics Plc,[31] using algorithms, initially to recognise the presence of a face, and secondly to

[30] DARPA, 2000
[31] http://www.visionics.com

determine the precise location of pre-defined features within the face. Image capture can occur from static frames, such as photographs taken of an incident, or from real-time moving faces on a CCTV video camera, allowing recognition to take place from a number of available resources. Many of these software applications are available to both public and private enterprises, which raises questions over who is able to operate surveillance systems and whether they are registered or monitored in relation to human rights issues.

The algorithm used is based upon the inner regions of the face, therefore, changes in hairstyle, colour or facial expression do not affect identification, thus avoiding some of the faults associated with Principal Component Analysis as discussed in the previous chapter. In addition, background lighting does not pose a threat to the recognition system, so long as some ambient lighting is present, allowing the camera to focus on the subject. Facial hair and accessories such as hats and spectacles are not part of the overall recognition analysis, which, along with hairstyle, are major distractors with human recognition,[32] thus having the potential to demonstrate a higher success rate than human recognition.

DMV Case Study

In the US, State Departments of Motor Vehicles (DMVs) are using software developed by Visionics and Polaroid, to prevent criminals from obtaining multiple licences under different names.[33] Not only are the false licences fraudulently used by criminals convicted of motoring offences, but illegal copies are also used as age verification by younger individuals who are under the minimum legal drinking age. By preventing anyone but the original licensee from being issued a duplicate licence, both aspects of fraud can be targeted using such a system.

Both graph matching and PCA may be employed to some extent with this type of verification procedure. As the images are standard sizes and contain full frontal views with similar lighting levels, principal component analysis can be used, although only at a basic level to prevent daily ageing and changes in hairstyle from becoming a distractor.

[32] Interview with Prof. V. Bruce
[33] http://download.idg.net/crd_system_80198.html

In use by 37 of the 50 American States, computerised identity verification is faster and more efficient than the previous manual checks made by the authorities. The Californian DMV database contains 400 million images, which would take over one hundred thousand man-hours to sift through on the basis of viewing one image per second, a task that could not be performed for every licence application. West Virginia chose to implement a facial recognition system principally due to the negative publicity and public disapproval of the alternative fingerprint identification system that was piloted in the state of Georgia. Fingerprinting was found to be stigmatising, generally associated with criminal offences rather than being used for a simple identity verification process.[34]

The project would also allow for the issue of driving licences from automatic dispensing points or by other unattended or untrained means, thus reducing the cost and improving the efficiency of the state DMV. Using this form of recognition technology, crime is detected as the applicant makes a fraudulent application and criminal offences such as under-age drinking and the use of aliases are subsequently prevented. This and many other identity verification systems have proved to be very successful with many of the system objectives being fulfilled.[35]

PROfile Case Study

Designed to aid crime detection, PROfile[36] is a computer software application for use by law enforcement agencies. Currently used by Thames Valley Police Force in the UK, it employs biometric analysis of the entire face to match unknown offenders with known custody records and to create picture-based crime pattern analyses.

The system works by logging events, which may be classified as a crime scene, based on CCTV pictures and witness evidence; or as a mugshot based on custody photographs and police records. Within each event, multiple persons and pictures of each person may be added separately, so for example, a bank robbery would be classified as one event, containing individual descriptions of the three men involved

[34] http://www.altlatainfoguide.com/repeal/
[35] Access Control Systems have possibly received the most success, as seen by Lau Technologies in Weschler, 1997. Pg 402.
[36] http://www.zeda-abm.com/products/profile.htm

and two pictures of each man - one full frontal shot and one side-view obtained from the bank's security cameras. The pictures are then used to create an algorithm for the face: markers are manually placed at given points on the face, which then generates a unique code for the face, as shown in figure 3. This form of recognition is similar to the graph matching system developed by Wiskott et al. and does not employ any of the principal component analysis techniques.

To improve the use of the program, an algorithm is able to convert near-front face geometry into full frontal facial equivalents, allowing a wider range of CCTV pictures to be used, as the criminal is not always looking directly at the camera. Searches can be performed against the custody records to find the nearest matching faces from the mugshots - a standard deviation figure gives some idea of how similar the matched mugshots are to the original picture. Even if the criminal is not in the custody records, their face may be linked with other events, thus identifying repeat offenders and possibly revealing some details about their *modus operandi* such as target areas or preferred type of weapon or getaway vehicle.

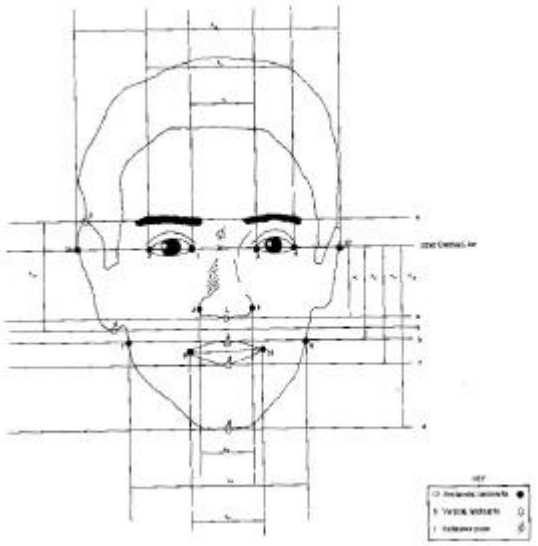

Figure 3. Set of landmarks for anterior analysis.[37]
The 12 horizontal and 6 vertical landmarks around the eyes, nose, ears and mouth are manually positioned, although the centre of each eye can be identified semi-automatically using Visionics Software.

[37] Adapted from Mardia et al., 1996

Further searches can be performed using a simple search engine, finding similar persons matching witness descriptions, or by looking for similar events such as bank robberies, or incidents that took place in the same area involving three persons. Crime pattern analysis can be performed to check for crime hot-spots or frequent times so that the police can allocate their resources accordingly. Such a search engine replaces the ideology of principal component analysis, as manually entered data such as 'dark collar-length hair' is a substitute for the pixel colour and distribution data.

PROfile acts as a form of crime detection tool by identifying individuals caught on CCTV and is able to search for related crimes. However, unlike the DMV case study, searching and recognition is not completely automatic, as a crime intelligence officer must enter the data into the system manually, adding the facial landmarks to each photograph to generate the algorithm to be used to compare the face against the other records. Future research into facial recognition may provide the ability for computers to recognise not only the face, but to be able to determine the location and relative size of the eyes, nose, mouth and other facial landmarks.

Mandrake Case Study

As crime prevention has been shown to be more significant in security issues, and that crime detection is of more significance to the police and other law enforcement agencies, amalgamating the two approaches to computerised recognition may provide a powerful solution to combat crime.

By combining both the automatic recognition technology of the DMV case study and the criminal databases of known criminals exploited by the PROfile system, much research has been undertaken to formulate a recognition system which can alarm the law enforcing agencies as to the presence of a known criminal. Many commercially and publicly funded ventures have involved such technology, the first CCTV and facial recognition system in the UK was instigated by the Metropolitan Police in Newham, East London.[38] Despite pressure from many civil liberties groups, the system named Mandrake is able to examine every passing face and alert the police

[38] As reported in the *Observer*, 11 October 1998

when a given individual is recognised from the police database. The system relies wholly on a graph matching system, analysing the area around the eyes and the nose which can be converted into an algorithm without any manual intervention that was necessary for the PROfile system.

However, placing high-quality security systems on the corner of every street would not be economically possible, although many councils have established CCTV networks covering most of the town centre and cover many areas susceptible to crime. Stockton-on-Tees, one of many UK cities to employ CCTV networks, has over 47 cameras in the centre alone and more cameras located in the residential areas of a town with less than 200,000 inhabitants.[39]

One of the many potential problems of an instant-alert system is that previously convicted petty criminals going about their daily business would be constantly 'recognised' and their presence would be relayed to the police. Society would feel that a major invasion of privacy had occurred, with their identity and exact location being too easily available to the police. To combat anxieties such as these, Newham Council gave as an example the way in which twelve known paedophiles in the area who would only be positively identified by cameras adjacent to the local schools. Thus, the daily movements of the known offenders were not continually monitored and their general privacy was not impinged upon. Internal checks administered by the law enforcement agency would cause records to be kept of who was to be targeted, who authorised the surveillance and what areas were to be covered.

By placing a surveillance system in a unique area and attaching a database specific to known criminals who would operate in that area, a reasonable successful hit rate can be achieved without infringing the general privacy of the public. From the example of the paedophiles put forward by Newham Council, other locations may be highlighted as target areas for particular types of offenders. Airports are prime examples of locations that are frequented by drug traffickers who will usually be 'on business' in such locations. Security cameras are a regular feature of airports and can easily be linked to a recognition system containing an appropriate police database.

[39] www.homeoffice.gov.uk/crimeprev/cctv.htm

The violence surrounding the Euro 2000 football games in the Netherlands was analysed through CCTV cameras. Recognition software was employed to alert the authorities to known troublemakers crossing border control points and to identify the main instigators of the riots. Experts found that their software recognised many individuals entering and leaving the country resulting in arrests by the Dutch authorities.[40]

[40] http://news6.thdo.bbc.co.uk/hi/english/euro2000/teams/england/newsid%5F796000/796242.stm

Chapter 4

Reliability

This chapter aims to analyse the reliability and accuracy of the technological processes and commercial products employing facial recognition.

Reliability of Automatic Facial Recognition

In 1998, the House of Lords Select Committee on the Submission of Digital Images as Evidence reported on the potential to change or manipulate digital images and records leaving little or no obvious sign of tampering.[41] Whilst the report was concerned with the validity of the images as a whole and of the quality of the picture, further problems arise concerning the reliability of identification from traditional and digital images. With both technological analysis and human judgement being involved in the process, the reliability of both human and automatic analysis of CCTV footage may be questioned.

By comparing computerised facial recognition with the counterpart models of human recognition, an assessment of the possibility to employ biometric identifiers has already been made. Whilst the previous chapter demonstrated that computers were indeed capable of automatically identifying and subsequently recognising human faces, the accuracy and reliability of facial recognition software has become increasingly important as computer technology plays an ever-increasing role in the modern courtroom.[42].

The software companies producing identification and recognition systems such as those highlighted in chapter two produce brochures and manuals effectively selling the product to interested parties. In-house testing can be extremely subjective, with

[41] Select Committee on Science and Technology, 5th Report
[42] Widdison, 1997

varying aims, goals and test data depending on the actual use and requirements of the tasks the algorithms were developed to perform. The accuracy and reliability of their products, however, can only be assessed by comparing the product with standardised references or samples and subjecting them to further analysis by independent bodies.

In 1996, the Californian Welfare Fraud Prevention Squad commissioned a report to examine the current techniques for biometric identification, with particular attention given to accuracy, closed and open search requirements and data collection error rates.[43] The report rejected facial recognition along with iris scan biometrics due to the lack of research and development at that time. Fingerprint analysis was recommended to the Californian authority, having open and closed search abilities, low data collection errors and a high user acceptance rate. The measurement of accuracy, however, was conducted in such a way that not only could two facial biometric applications be compared, but they could also be assessed against other systems employing hand geometry, retinal and iris scans, fingerprint and other biometric algorithms.

Firstly, the rate of false acceptance was calculated from the number of occurrences where an individual is wrongly accepted as a match, and secondly, the rate of false rejects was recorded when the system failed to recognise a legitimate match. Creating a graph of both values as a function of the threshold for recognition, the point where the two error rates intersect was taken as the accuracy of the system: the greater the cross-over value, the greater the inherent accuracy of the system. This type of assessment could then compare different techniques to select the most appropriate approach to combat a given problem. This independent analysis was also free from the bias and propensity of company sales literature.

The FERET Programme

In 1996 the FERET Verification Testing Protocol for Face Recognition Algorithms was devised to provide an accurate and independent assessment of the reliability and accuracy of existing facial recognition systems. It also served to promote research in

[43] Prepared by The Biometric Consulting Group. http://www.bioconsulting.com/bio.htm

facial biometrics in academic and public / private sector industry, sponsored by the U.S. Department of Defense Counter-drug Technology Development Program.[44]

A Target set containing a gallery of 'known individuals' and a Query set of 'unknown faces' were presented to participating software produces in September 1996. Two version tests were administered: the first assessed automatic facial location, and the second version provided eye co-ordinates to assess the recognition performance of manual input systems. Enrolment and test data was collected according to strict guidelines to enable a fair comparison to be made. A scoring procedure was devised based on ROC graphs, originally devised for SONAR false recognition rates.

Receiver Operating Characteristic (ROC) curves employ similar 'failure to enroll' and 'failure to acquire' rates to the Californian report. False match rate and false non-match rate were plotted on log-log scales as shown in figures 1 and 2.

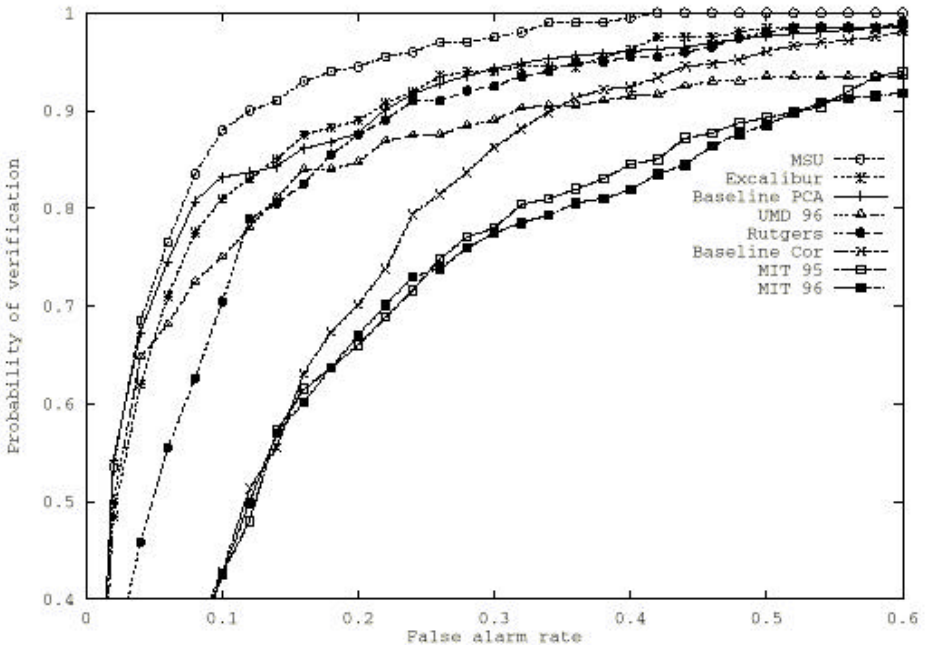

Figure 4. A ROC curve from September 1996.[45]

Note that to achieve a recognition probability of >90%, the system will exhibit a higher false alarm rate: the best system having a 10% false alarm rate, with others varying from 30 to 60%. By reducing the false alarm rate, the general trend was a reduction in verification probability.

[44] Phillips et al., 1997

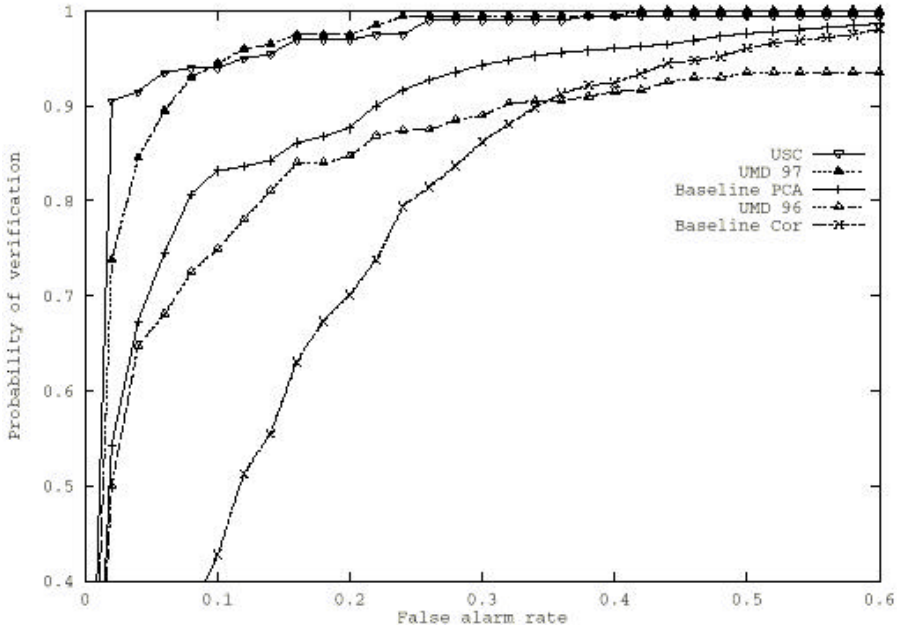

Figure 5. A ROC curve from March 1997.

Over six months, the >90% recognition rate using the same FERET protocol exhibited a general reduction in false alarm rates. The best system exhibited < 2% false alarm rates, with others varying from 20 - 30%. This gave the system an increased recognition probability with no significant increase in false alarm rates.

Further tests were performed until March 1997, when the Department of Defense published details of their results for the whole project. A significant increase in performance was seen for the general field of facial biometric comparison and for individual algorithm-based systems. Strengths and weaknesses of individual algorithms were highlighted to facilitate further research to promote and improve the use of facial biometrics. However, it was evident that further research was still required if facial biometrics were to compete with other forms of biometric identification, even though progress had been made in these areas over six months

A major fault of face recognition algorithms appeared to be sensitivity to variations in illumination caused by the change in sunlight intensities throughout the day. As shown by table 1, changing the illumination resulted in a significant performance drop. For some algorithms, this drop was equivalent to comparing images taken over the course of a year and a half apart.

[45] Figures 1 and 2 adapted from Rizvi et al, 1998

Table 1. Results for the FERET test for the best algorithms in each category.

Category	False alarm rate (%)	False reject rate (%)
Same day, same illumination	2	0.4
Same day, different illumination	2	9
Different days	2	11
Different days over 1.5 years apart	2	43

In addition, the position of the target face may also affect performance. A 15-degree difference in position between the query image and the database image creates a significant difference in the recognition threshold, and a difference of 45 degrees renders the system ineffective for recognition.

These results give facial biometrics a disadvantage over other identifiers; however, by identifying the weaknesses further improvements may be seen in the future. Despite the limitations from luminosity and face position, the process of identification was proven as successful and provides some useful resources to the field of law enforcement.

FRVT 2000

With significant improvement in the development of facial algorithms for computerised recognition since the FERET programme, the capabilities of modern technology is in need of re-assessment. A new set of evaluations was set up by the Department of Defense as the Facial Recognition Vendor Test (FRVT) 2000.[46] Administered in May - June 2000, the FRVT 2000 will provide the most up-to-date analysis of facial recognition. Significant improvement is expected for individual algorithms and computer systems, but it remains to be seen whether facial biometrics will be as effective or accurate as fingerprint analysis. With recognition performance and product usability being tested, it is likely that facial recognition software will receive a hallmark of approval and will cease to be dismissed from reports such as the Californian Welfare Fraud Prevention investigation into biometric techniques.

[46] http://www.dodcounterdrug.com/facialrecognition/FRVT2000/frvt2000.htm

Chapter 5

Justice

This chapter will explore and expose the possibilities for mistakes, mis-use and abuse of identification through facial recognition and biometric comparisons.

Potential for Miscarriages of Justice

The previous chapter analysed the reliability of computer-mediated recognition and assessed the apparent success rate of automatic facial recognition. The potential for errors within computerised systems in a legal environment raises concern for judicial mistakes, whether the systems in question are fully automated or directed by human supervision.

The Use of Statistics in Evidence

The analysis of the reliability of facial biometric systems provides an assessment based on percentages, probability and other statistical measurements. Redmayne[47] highlighted the key question of 'Can liability be based on naked statistical evidence?' Whilst evidence from an expert witness, based around scientific analysis, opinion and statistics, is admissible in the UK, the Supreme Court in Minnesota held that scientific evidence should not be presented in probabilistic terms.[48] The decision from the more recent case of State v. Bloom[49] held an exemption to the no probability rule. DNA test results expressed in probabilistic terms were permitted as evidence, principally due to the reliability of testing and the unique composition of DNA amongst individuals. However, the principal problems with presenting evidence in terms of probability is universal and relies more on the interpretation of statistics rather than the techniques used to obtain them.

[47] Redmayne, 2000

As facial biometric analysis relies on algorithmic searching of unique identifiers, the matching of an individual's mugshot with a crime scene photograph can be expressed in terms of probability. This occurs not only with facial biometrics, but with fingerprint matching, blood and semen analysis and most other types of forensic evidence. Explaining probability to the jury has been questioned at the Court of Appeal with no unproblematic solutions emerging. In the UK, R v. Deen[50] highlighted the difference between two confusing questions posed by the prosecution and the defence:

1. What is the probability of finding the evidence, given that the defendant is innocent?
2. What is the probability that the defendant is innocent, given the evidence?

In other terms, if there is a 1:3 million probability that suspect A is the face on the CCTV footage of an assault, it does not mean that there is a 1:3 million probability that A committed the crime. Explaining the implications of probability to the jury is not an easy task, particularly when both the prosecution and the defence will present the evidence to favour their case.

The first question only proves that there is a high degree of similarity between the suspect and the assailant. This question should be answered by the expert witness based on statistical evidence and is analogous to an identity parade with an eye witness.

The second question should be put to the jury with appropriate direction by the judge presiding over the case. The probability of innocence must take any other pieces of evidence into account and also examine the likelihood of other individuals matching the assailant's biometrics. In R v. Deen, the Lord Chief Justice stated:

> "It makes it very difficult, even if the scientist gets it right, and the judge gets it right - if this is what is right - what on earth does an ordinary jury make of it?"

---

[48] State v. Carlson [1978] 267 NW 2d 170; State v. Boyd [1983] 331 NW 2d 480
[49] State v. Bloom [1994] 331 NW 2d 159
[50] R v. Deen [1994] The Times, January 10 1994

A Bayesian model[51] for combining evidence has been formulated and was tested in R v. Adams.[52] A database search linked Adams with a rape assault, the linkage being the only piece of evidence from the prosecution. All other evidence favoured Adams, including failure by the victim to identify Adams; failure to match the description given to the police at the time of assault; and an alibi provided by Adams' girlfriend. Adams was convicted at the court of first instance, however, an expert witness from the defence explained how to apply Bayes' Theorem to the jury. An appeal was granted as the judge failed to explain the Bayesian method clearly in the summing up, however, the Court of Appeal quashed the conviction but criticised Bayes' Theorem. A re-trial was ordered, and the conviction was held.

Several attempts to convert statistics into more manageable or significant terms for the jury have been made, including translating numbers into a verbal scale of probability. Although this allows a better comparison of cases and makes presentation easier, the scheme lacks precision and may be interpreted differently as words can have different meaning for each individual.

The Technological Revolution

The primary cause for concern with technology *per se* arises from the interconnectivity of cameras, computers and databases between private companies, national police agencies, and international law enforcers. Whilst this allows for swift and effective exchange of data to improve and update resources, it also amplifies and distributes the data that has been gathered:

> *"Now through the database alone, the subject has been multiplied and decentred, capable of being acted upon by computers at many social locations without the least awareness by the individual concerned"*[53]

Serious problems arises when erroneous or false entries are made on one database, which are then carried around the network of computers and databases, replicated many times over. These mistakes, even when they are identified may be difficult to

[51] As described in Redmayne, 2000
[52] R v. Adams [1996] The Times, August 14 1996

completely eradicate from the entire network due to the back-up and assimilation capabilities of modern technology. One such example occurred when two British football fans were wrongly deported from Belgium due to a database error - a six-year campaign revealed that their names were still entered on some national databases describing the individuals as football hooligans despite having been removed completely from the Belgian database.[54]

Networking databases raises problems of rights to access information concerning the individual, which are often brushed away by State Security Services under the guise of 'National Interests' to remain immune from data protection laws, judicial scrutiny, legal or political accountability. There is an obvious danger that police records could move towards this type of immunity, however, the laws on court procedure, evidence-handling, etc. will maintain the necessary checks on the validity of data. Restricting database access can prevent mis-use by implementing a user request service with authorisation coming from a higher ranking officer, however, increased beaurocracy will ultimately cause delays in finding relevant information. The EU have proposed model for investigation management that will electronically log who accessed the database, for what purpose, who gave authorisation and what data was viewed added or removed.[55]

Although the human rights of the innocent must be upheld, there will be an increasing danger of criminals escaping conviction on technicalities designed to prevent police and judicial investigations from abusing both public and private databases. The right to privacy must occasionally be stretched to allow investigating authorities to invade that privacy on a minor level to prevent a more serious crime of rape or assault from occurring in the future.

Entering facial biometric data into networked databases can ultimately permit a user to locate a known individual through CCTV cameras as discussed in relation to the Mandrake system. With other biometric identifiers, such as fingerprints or DNA / blood analysis, it is only possible to link to an individual after the crime has occurred and the prints have been lifted and recorded on the database. With facial biometrics

[53] Poster 1996, pg 185
[54] Statewatch, Mar/Apr 1993; Jul/Aug 1996

a suspect can be located before any further crimes are committed provided the suspect enters territory covered by a camera. Whilst this may be useful for the arrest of a wanted suspect and prevent further crimes occurring, using such a system to locate an individual on the basis of suspicion or without any warrant to do so would be severely abusing the position of power the official has through access to the database.

The principle of presumed innocence would be breached by such fishing expeditions; by implementing database access controls, restrictions, user management log checks and other regulatory practices, such unlawful use can be restricted but never fully eradicated.

Discrimination

Further potential for the miscarriage of justice lies in the domain of discrimination: not only racially, but also socially and financially. CCTV surveillance is generally conducted by human operators, as computerised systems are not yet capable of recognising or recording deviant behaviour. The subsequent analysis or recognition of the deviant may be carried out automatically without any aid from the human operator.

From studies into the use of CCTV, Dr Clive Norris of the Centre for Criminology and Criminal Justice at Hull University[56], found that:

?? 40% of people were targeted for "no obvious reason", mainly "on the basis of belonging to a particular or subcultural group". "Black people were between one-and-a-half and two-and-a-half times more likely to be surveilled than one would expect from their presence in the population".

?? 30% of targeted surveillances on black people were protracted, lasting 9 minutes or more, compared with just 10% on white people.

[55] Tupman, 1998
[56] Norris & Armstrong, 1997

?? People were selected primarily on the basis of "the operators negative attitudes towards male youth in general and black male youth in particular. …[I]f a youth was categorised as a 'scrote' they were subject to prolonged and intensive surveillance."

?? Those deemed to be "out of time and out of place" with the commercial image of the city centre streets were subjected to prolonged surveillance. "Thus drunks, beggars, the homeless, street traders were all subject to intense surveillance".

?? Finally, "anyone who directly challenged, by gesture or deed, the right of the cameras to monitor them was especially subject to targeting".

However, the general prejudices and discriminatory trends of the CCTV operators may be simplified into rules that can be followed by the most simple automated decision making system. Whilst motion and heat detectors may be 'blind' to race and gender, the processing of digital images can distinguish between black and white, and through algorithmic processing, future developments may be able to differential between male and female, young and old. No laws exist to restrict the use of discriminatory algorithms, as many banks and credit companies utilise such automated processes for credit applications.

The Church Case

The appeal cases of R v. Church[57] and Church v. HM Advocate[58] revolved around the admissibility and materiality of additional evidence concerning expert evidence on facial identification. The case has been recently referred to the new Scottish Criminal Case Review Commission[59] for further consideration. Although the main grounds for appeal were concerned with why further expert evidence was not adduced and whether the absence of funding through legal aid was a reasonable excuse, conflicting opinions were given concerning identification through facial mapping.

[57] [1995] 2All ER 72
[58] [1995] SLT 604-611; [1996] SLT 383-385
[59] www.sccrc.org.uk

The High Court[60] heard that the results of a comparison of a photograph of the accused and the video footage of the attack were inconclusive.[61] Further comparisons were recommended but not prepared due to insufficient funds. Despite the positive identification of the suspect by four eyewitnesses, the appeal was granted and a second biometric comparison was commissioned. By August 1994, expert evidence[62] identified significant differences between the images of the assailant and the accused, concluding that the appellant's face did not match that of the robber. Further examination of the evidence, on the instructions of the Lord Advocate, resulted in further expert evidence stating that the video imagery was of too poor quality to be of any use for biometric analysis and photographic comparison.[63] Following a further trial the accused was again found guilty.

This case saw conflicting opinions from several experts in the field of facial identification, biometric analysis and facial mapping, some of whom had developed expertise through experience rather than scientific training. With ongoing appeal at the Review Commission, this case will no doubt be used as an example for future cases, causing expert evidence in the field of facial identification to be called into question. The opinion of the Review Commission will no doubt set a precedent in this field, however, they must be careful not to damage the progress made by technology in the legal environment without serious thought as to the future of facial recognition.

Profiling

Although not a direct concern to facial recognition technology, Effross[64] raises concern over the profiling of normal everyday persons, who, perhaps, frequent certain locations more often then others. The profiling of known criminals is considered acceptable, as its primary aim is to provide evidence that will lead to the arrest of a criminal. Since the process of data collection and the building of profiles can be done automatically, there is the potential to allow profiles of most individuals

[60] High Court in Glasgow June 8 1994
[61] Report by Dr. Bowie
[62] Report by Drs. Linney and Coombes
[63] Report by Dr. Sandham
[64] Effross, 1999

to be constructed: the only limiting factor being the time taken to download and store the data that the computer has created.

Traditionally, police officer-based surveillance is only carried out when the detective team have sufficient evidence or 'instinct' to warrant the time and expense taken to set up such an undercover operation. With automatic profiling, there is no need for any number of persons to be present, and previous movements of the suspect may be drawn from archived data from the previous week, month, or even year.

Not only are the police able to construct and use personal profiles, but the abilities of the private sector are also increasing to allow profiles of customers and visitors to their premises both in the real world and in virtual reality through 'Trojan Horses' and 'Cookie' technology. The records of what we buy and what sites we visit may be argued as private and personal information which should not be disclosed or as useful information to the vendor provided that they do not abuse the data that they have collected. Commerce has the technology to record the transactions we make through electronic points of sale (EPOS), credit and debit cards, supermarket loyalty cards etc. for a number of years, with presumed consent to pass on your details to third parties unless you tick the small box at the bottom of the page.

It is doubtful as to whether pictoral profiling of people during everyday events by private enterprises will ever be accepted as ethical practice for commercial purposes or even for police access either as a resource or connected via a computer database linkage. Police access to health records has been a controversial area, primarily due to the health care professionals' guarantee of privacy to their patients; police access has so far been on an *ad hoc* basis with the health authorities requiring convincing reasons for their disclosure.

Banks, also, will act in the interests of their customer to protect their privacy without substantial justification for police investigations, however, the owners of CCTV archives will generally be supermarkets, local councils, retailers and other private enterprises with less regard for the rights of privacy of the individuals who frequent their premises. Quite often, a retailer would gladly offer CCTV footage to police enquiries as the apprehension of criminals or even potential offenders would be to

their advantage. The sole reason for the existence of CCTV in their premised is to detect and discourage theft or damage to their property or merchandise.

Chapter 6

The Future

Future developments and the legal decisions surrounding facial biometric analysis cannot be easily anticipated. This chapter will examine some future uses for recognition systems and provide some conclusions from the previous chapters.

A Legal Tool

From the number of criminal cases involving facial identification experts, it is almost certain that any developments in the field of computerised facial recognition will be explored and utilised by the legal profession. Their exact use and reliability will vary from system to system, however, police forces have already established Information Technology divisions and have drawn their resources together to provide an easier and more accessible flow of information. The value attached to the output of computerised identification systems will need to be decided by the operators and the legal weighting as evidence will continue to be decided by the judge and jury.

DARPA Project

The Defense Advanced Research Projects Agency (DARPA) initiated a research program to encourage developments in computerised human identification from a distance. The first part of the project initiated in August 2000 will include an assessment of current technology that will most likely show that facial biometrics have the required potential to develop further for distant recognition. Important research areas have been highlighted such as multiple biometric sensors, investigations into luminosity and weather conditions and three-dimensional analysis. Phase two, scheduled for 2002, will concentrate on improving the current algorithms to identify cooperative, non-cooperative and un-cooperative targets and extending their target range to an ultimate goal of 500ft (just under 1km).

Compared to the FERET and FRVT 2000 tests, this project aims to promote the development of facial recognition technology as well as providing more accurate and reliable biometric systems, extending surveillance capabilities and overcoming the current problems associated with facial recognition, as outlined in previous chapters.

Such developments are promising for all of the academic and public / private interests in computerised facial recognition. The enhancement of reliability and user acceptance will augment and consolidate the legal acceptance of such technology whilst current criminal cases provide the juridical precedents for future litigation.

References

Bruce, V and A Young (1986). Understanding Face Recognition. *British Journal of Psychology*. **77** 305-327

Bruce, V (1994). Stability from Variation: The Case of Face Recognition. The M. D. Vernon Memorial Lecture. *The Quarterly Journal of Experimental Psychology*. **47A (1)** 5-28

Defense Agency Research Projects Agency (DARPA) (2000). Human Identification and a Distance. Proposer Information Pamphlet. 10th February 2000

Daugman, J (1997). Phenotypic Versus Genotypic Approaches to Face Recognition. In *Face Recognition From Theory to Applications*. Ed. H. Wechsler. Springer-Verlag Berlin.

Dukantas, P (1999). The Service Wants to Eliminate Passwords for Verifying Users. *Government Computer News*. **118 (**32)

Ellis, H; Shepherd, J and G Davies (1979). Identification of Familiar and Unfamiliar Faces from Internal and External Features. *Perception*. **8** 431-9

Effross, W (1999). Commercial Profiles vs. Suspect Classifications: Preparing, Preventing and Parrying Public and Private Profiling, *Presented in New Orleans at the Association of American Law Schools' Annual Meeting, at a joint program of the Computers and Law and the Privacy of Defamations Sections 1999*. Published on-line by the Stanford Journal of Law and Technology in March 1999

Faw, H (1992). Recognition of Unfamiliar Faces: Procedural and Methodological Considerations. *British Journal of Psychology*. **81** (3) 25

Hancock, P; Bruce, V and A Burton (1998). A Comparison of Two Computer-based Face Identification Systems with Human Perceptions of Faces. *Vision Research*. **38** (15/16) 2277

Hill, H and V Bruce (1993). An Investigation into the effects of lighting and viewpoint on face processing with with the use of a simultaneous matching task. Paper presented to the 16th European Conference on Visual Perception, Edinburgh. *Perception*. **22S** 22-23

Huxley, A (1955). Brave New World. Chatto and Windus. London

Klatzky, L and H Forrest (1984). Recognising Familiar and Unfamiliar Faces. *Memory and Cognition*. **12** (1) 60-70

Lyon, D (1991). Bentham's Panopticon. *Queen's Quarterly*. **3** 98

Lyon, D (1994). The Electronic Eye: The Rise of surveillance Society. Polity Press. Cambridge

Lyon, D and E Zureik (1996). Computers, Surveillance and Privacy. University of Minnesota Press. MN

Norris, C and G Armstrong (1997). The Unforgiving Eye: CCTV Surveillance in Public Space. http://merlin.legend.org.uk/~brs/archive/stories97/suspects.html

Orwell, G (1954). Nineteen Eighty-Four. Harmondsworth: Penguin. London

Pentland, A; Moshaddam, B and T Starber (1993). View-based and Modular Eigenfaces for Face Recognition. *Proceeding of IEEE Conference on Computerised Vision and Pattern Recognition 1994*. 84-91

Phillips, P; Moon, H; Rizvi, S and P Rauss (1997). The FERET Evaluation. In *Face Recognition from Theory to Applications*. Ed. H. Wechsler. Springer-Verlag Berlin

Poster, M (1996). Database as Discourse; or, Electronic Interpellations. In *Computers, Surveillance and Privacy*. Ed. D. Lyon. University of Minnesota Press. MN

Redmayne, M (2000). Presenting Probability in Court: The DNA Experience. *International Journal of Evidence and Proof*. **1(4)** 187

Rizvi, S; Phillips, P and H Moon (1998). The FERET Verification Testing Protocol for Face Recognition Algorithms. National Institute of Standards and Technology. Technical Report 6281

Tupman, W (1998). The Use of Criminological Data in Police and Judicial Investigation. Presented to the XXth Police Course of Higher Specialisation, Catania, October 1998.

Turk, M and A Pentland (1991). Eigenfaces for Recognition. *Journal of Cognitive Neuroscience*. **3** 71-86

Valentine, T and V Bruce (1986). Recognising Familiar Faces: The Role of Distinctiveness and Familiarity. *Canadian Journal of Psychology*. **40** (3) 300-305

Widdison, R (1997). Beyond Woolf: The Virtual Court House. *Web Journal of Current Legal Issues*. http://webjcli.ncl.ac.uk/1997/issue2/widdison2.html

Wiskott, L; Fellous, J; Kruger, N and C von der Malsburg (1995). Face Recognition and Gender determination. *Proceedings of the International Workshop on Automatic Face and Gesture Recognition*. Zurich 1995

Young, A; Hay, D and A Ellis (1985). The Faces that Launched a Thousand Slips: Everyday Difficulties and Errors in Recognising People. *British Journal of Psychology*. **76** 495-523

Zhao, W; Krishnaswamy, A; Chellapa, R; Swets, D and J Weng (1997). Discriminant Analysis of Principal Components for Face Recognition. In *Face Recognition from Theory to Applications*. Ed. H. Wechsler. Springer-Verlag Berlin

Acknowledgements

I would like to thank the following people who contributed to this dissertation:

Mr.Burkhard Schäfer - Edinburgh University Law Faculty - for supervision, guidance and comments on my first drafts.

Prof. Vicki Bruce - Stirling University Psychology Department - for many useful comments and references during an interview 30/08/00.

Dr. Leslie Bowie - ABM (UK) Ltd - for providing details of biometric systems and reliability tests.

Mr. Thomas Ruggles - California SFIS Technical Consultant - for comments on the comparison of biometric techniques.

Stephanie, my family and friends for their support throughout my study.