LAW ENFORCEMENT MANAGEMENT INSTITUTE

# BIOMETRICS: A SOLUTION TO DRIVER LICENSE DOCUMENT FRAUD

A RESEARCH PAPER

SUBMITTED IN FULFILLMENT

OF THE REQUIREMENTS FOR

MODULE III

BY

ROBERT H. BURROUGHS

TEXAS WOMAN'S UNIVERSITY
RECEIVED
NOV 20 1991
LAW ENFORCEMENT MANAGEMENT INSTITUTE

TEXAS DEPARTMENT OF PUBLIC SAFETY

SULPHUR SPRINGS, TEXAS

NOVEMBER, 1991

#31

## Statement of Purpose

It is my intention in this writing to examine some of the economic and social costs of fraudulently obtained driver licenses and identification certificates. Furthermore, it will be the purpose of this paper to discuss the technology available to curb this problem and make a comparative analysis of the technologies which hold the greatest promise for utilization in the driver licensing environment.

TABLE OF CONTENTS

Statement of Purpose . . . . . ii

Table of Contents . . . . . .iii

List of Tables . . . . . .iv

List of Figures . . . . . .v

Chapter

1. The Problem of Document Fraud . . . . . 1

2. Biometric Identification . . . . . 6

3. Biometric Technologies: Identified and Described . 9

Behavioral Biometric Identifiers

Physiological Biometric Identifiers

4. Biometric Technologies in the Driver License Environment . . . . . 16

Social Issues

Legal Issuses

5. Biometric Technology Evaluation . . . . . 26

Retina Scan Method and System Analysis

Automated Fingerprint Method and System Analysis

6. Automated Fingerprint / Retina Scan Analysis . . . 38

7. Conclusions . . . . . 42

Endnotes . . . . . 44

Works Cited . . . . . 47

Cases Cited . . . . . 49

## LIST OF TABLES

Table Page

1. Response Percentages of Biometric Sampling Questionnaires . . . . . .18

2. Reasons for nonparticipation in Biometric Sampling . . . . . .20

3. Test Results of Retina Scan Accuracy . . . . . .28

4. Data Processing Response Time for Retina Scanning Tests . . . . . .28

5. Test Results for Automated Fingerprinting Accuracy. 34

6. Data Processing Response Time for Automated Fingerprinting Tests. . . . . 35

## List of Figures

Figure Page

1. Orkand Corporation, "Personal Identifier Project", Final Technical Report, 1990 . . . . . 27

2. Fingermatrix Incorporated, Fingermatrix Fingerprint Identification Technology (An Overview), 1988 . . 32

3. Fingermatrix Incorporated, Fingermatrix Fingerprint Identification Technology (An Overview), 1988 . . 32

# CHAPTER 1

## The Problem of Document Fraud

The problem of document fraud is demonstrated by the number of driver licenses and identification certificates issued in the State of Texas which are fictitious. It is estimated that fifteen percent of all issued driver licenses and identification certificates are fraudulent. It was further stated that four million driver licenses and one million identification certificates issued in Texas are fraudulent. The major problem with this immense number of fraudulently obtained documents is that the driver license or identification certificate is considered to be "de facto" identification in the United States. These documents hold a much greater degree of credibility than is justified by current security and control measures.[1] Current licensing identification procedures leave a great deal to be desired in terms of validity and integrity. While these licensing programs require positive identity, current systems do not provide integrity of individual issued documents.[2]

The driver license or identification certificate is issued with a "positive" identification document such as a birth certificate, passport, baptismal certificate, alien

registration card, or school transcript. These documents generally must have an official seal or notarization attached to be acceptable. When such authorization is supplied the document is considered valid on its face unless the licensing employee has knowledge that the document has been tampered with or is fictitious. This identification system is not foolproof and never can be. Consequently, a person may apply for many driver licenses or identification certificates in several names, by obtaining identifying documents in several different names.

The most common fraudulent document is the birth certificate. These certificates can be illegally obtained, forged, or altered. The certificate is presented and a driver license or identification certificate is obtained which opens the door for the person to commit criminal offenses ranging from alcohol abuse, to large scale theft, to change of identity to evade arrest on other charges. The birth certificate of a deceased person is obtained for this purpose and since birth and death records are rarely compared it is relatively easy to assume the identity of a deceased person.[3] Another common problem is that a forged birth certificate is relatively easy to use since the birth certificate is rarely verified with the issuing governmental agency. An altered birth certificate is not easily detected when a photostatic copy is presented for a driver license or

identification certificate. The use of photostatic copies of birth certificates is currently acceptable to the Texas Department of Public Safety.[4] This policy requires the acceptance of the copied certificate unless there is an articulable reason to doubt the authenticity of the information contained on the certificate.

The consequences of fraudulently obtained driver licenses and identification certificates are astronomical in both physical and financial terms. Physical consequences include death and injury, while financial consequences cover only monetary losses.

Physical consequences can be enumerated in a variety of circumstances. However, the "Driving While Intoxicated" accident records of drivers between the ages of fifteen and nineteen are a nominal indicator of the scope of the problem. In Texas in 1989 there were 5,179 accidents in which 154 persons were killed and another 2,876 were injured.[5] In 1990 the total number of accidents was 5,049 in which 156 persons were killed and 2,877 were injured.[6] While these figures indicate a pervasive problem of under age persons consuming alcoholic beverages, there is no data to determine the number of under age alcohol abusers who obtained alcoholic beverages utilizing a fictitious driver license or identification certificate. However, these

persons assuredly contribute to this problem.

Along with the suffering and financial loss described above, there is another area of financial loss attributed to fraudulent identification the scope of which is staggering. The economic loss through financial institutions is estimated to range from 46 to 25 billion dollars in the United States annually[7,8]. The loss in the State of Texas is thought to range from 1.2 - 5.5 billion dollars annually. In Harris county in 1986 the loss attributed to fraud was 3.2 billion dollars. Of that amount twelve percent is directly attributable to false identification which translates to a total dollar amount of 384 million. Furthermore, in the same year in Harris county ten million dollars worth of dishonored checks were not prosecutable due to being issued by persons with fraudulent identification.[9]

These suffering and economic figures demonstrate a problem which has no foolproof cure. However, there is existing technology which can be implemented into the current driver licensing system which will greatly curtail the abuses existing in the current system.

Currently there is very little cross referencing of driver licenses, birth certificates, and social security numbers. Furthermore, there is no way of determining that

the person using any of these documents is entitled to them. To further complicate this delimma, the driver license and/or social security number is often used to regulate firearm sales, investigate crimes, identify subjects, and administer governmental programs.[10]

The challenge is to identify and implement a system which will establish and verify the identity of a subject.[11] The system must contain an unalterable identifier and would best be incorporated into the driver licensing environment. It is the concensus agreement that the driver licensing process is the best opportunity to perfect the identity of an individual.[12] The system alluded to is biometric identification.

## CHAPTER 2

## Biometric Identification

Biometrics is defined as the statistical study of biological observations or phenomena.[13] While this definition is correct, a better definition would be "a measurable physical characteristic or personality trait used to recognize the identity or verify the claimed identity of persons through automated means".[14] This definition better suits the technologies which will be discussed in this writing.

The principle of biometric identification is not new. It was used in prehistoric times to identify persons and animals by the trail they left. A hunter would identify his quarry by the size, shape, depth, length of gait, or other unusual characteristic of the impression which was left. Modern biometric identification however began in the United Sates in 1903 when the fingerprint was widely recognize as a unique identifier.[15]

Since 1903 The technology of fingerprinting went largely unchanged until the 1970's when the automated

fingerprint identification system was conceived as well as other automated biometric technologies. In the 1980's these technologies were born and will mature in the 1990's. The field of biometrics has achieved its present level of sophistication and application with astounding quickness. Biometric technologies pick out the various individual characteristics through microchip processes and reduce these to digitized codes which are compared to existing records in a database. This comparison is performed very quickly and returns with an infinitesimal error factor.[16]

Historically biometric technologies have been utilized in the security access field. Various technologies have been utilized as "keys" to secured areas, buildings, military facilities, and computer data. Currently however, these technologies are used to ensure hospital patient identities, identify incarcerated persons, control public welfare services, and provide positive identity in situations where such is imperative. The day is not far off when biometric technologies will be utilized in consumer markets such as automated tellers, and in thwarting white collar computer crime which is estimated to cost United States businesses 46 billion dollars annually.[17]

The sophistication of biometric technologies has risen to the level that computers can recognize an operator by the

way he types on a keyboard. Automated fingerprint scanners can determine if the scan is being made on a live subject or a deceased person. It is believed that biometric technologies will become essential in routine business expenditures in The 1990's. The reasons for reluctance in moving to biometric technology systems are, with the exception of fingerprinting, that they have not been widely accepted, they have had limited applications and have been rather costly. On the other hand, in our increasingly information based society, security must be maintained through "keys" which cannot be lost, stolen, duplicated, or overheard and offer a potentially foolproof identification.

# CHAPTER 3

## Biometric Technologies: Identified and Described

A biometric identifier positively identifies an individual independent of any other information which is supplied by the individual. Biometric identifiers are physical or behavioral traits which cannot be changed at will and would prevent two people from being identified by the same identifier. In essence, a biometric identifier is a unique trait that needs only to be measured, recorded and stored for future reference. Identity verification is based on a high degree of correlation in matching a known set of measurements to a subsequent set. Any biometric technology should be capable of verifying and enrolling applicants, serving a large database, and allowing monitoring of the biometric sample collection.[18]

Biometric identifiers are divided into two categories: behavioral and physical.[19]

### Behavioral Biometric Identifiers

Behavioral identifiers include:

- voice characteristics.
- signature dynamics[20].
- typing dynamics[21].
- golf swing dynamics[22].

The voice characteristic technology measures vocal pitch, volume and resonance. As many as fourteen vocal characteristics can be measured including the amount of air emitted from the mouth. This feature is to defeat the use of vocal recordings to break the identification system code. Voice measuring instruments are user friendly and inobtrusive to persons. However, these systems only perform verification of a known vocal print and do not enroll new "prints" automatically. Furthermore, vocal characteristics vary according to a person's mood or physical condition which causes some false rejections of an individual.[23] This system requires a high degree of user cooperation and has too great a potential for false rejections to suit the needs of the driver licensing environment.

The signature dynamic biometric technology is not based on handwriting. This system assesses the rate of movement, direction, pressure, and interruptions of an individual signing his name. This process evaluates and measures the motion of the signature not the final result. Hence, a

forger may be able to replicate the final result but not the process. Signature dynamic recording instruments are also user friendly and inobtrusive but they have the same drawbacks as voice scanners in that they only verify identity and do not provide an enrollment function for adding non-matching records to those currently in the database. Further detractors to this technology include the fact that dynamics change with name changes and when the name is written with the opposite hand. This identification system is totally dependent upon user cooperation[24] and would, therefore, be unacceptable in the driver licensing environment.

The typing dynamic technology measures the pressure, rate, and pauses of a particular entry on a keyboard. The keyboard "senses" if the authorized user is logging onto the system.[25] This system operates on the same principle as the signature dynamic system and has many of the same drawbacks. The dynamics are effected by the user's physical or emotional condition, typing skill level, and his control over the access code. This technology is totally dependent upon the user's cooperation and is only user friendly to persons with keyboard experience. Since this a relatively new technology no data supports this but, it is my opinion, only persons with routine keyboard experience could be identified by this system with any degree of accuracy. This

system is also a verification system and does not meet the enrollment needs of the driver licensing environment. Therefore, this technology would be unacceptable for driver licensing purposes.

The golf swing dynamic[26] is mentioned only to illustrate the many individual behavioral characteristics which are currently being examined. This technology measures the motion of the club swing and, thus, would be completely dependent upon user cooperation. Obviously, there would be no practical application of this technology in the driver licensing environment.

All the behavioral biometric technologies are not considered viable for driver licensing purposes because they are all verification systems and they each require a high degree of user cooperation as has been previously mentioned. The major problem with verification technologies is that they do not automatically enlarge an existing database which is a desirable feature in a driver licensing biometric identification system.[27] Furthermore, a biometric identification system should not rely heavily upon user cooperation nor should this system be dependent upon characteristics which are readily alterable. Behavior is not a constant factor and can be altered at will or by physical or emotional conditions which could result in a

false rejection rate that would be unacceptably high.[28] Thus, behavioral biometric identification systems do not meet the goal of a biometric identification system for driver licensing which is to obtain a positive identifier on all persons who are issued a driver license or identification certificate.

**Physiological Biometric Identifiers**

Physiological Biometric Technologies include:

- Hand Geometry[29].
- DNA Fingerprints[30].
- Fingerprints.
- Retina Scan[31].

Hand geometry technology measures several characteristics of the hand including palm size, finger length and width, and any unusual hand configuration. The hand geometry technology is an identification verification system and does have the capability of enrolling new subjects. Another disadvantage of hand geometry is that the hand is affected by jewelry, fingernail polish, injury, and disease.[32] These negative factors render this technology unsuitable for the driver license environment due to the possibility of an unacceptably high rate of false rejections.

DNA fingerprinting is the latest and most accurate biometric technology to date. DNA technology profiles one or more rare features of the individual's genetic pattern. The only genetic patterns which are similar are those of identical twins and there are even minor variations between these. An individual's DNA pattern is replicated exactly in all cells in the body and remains constant throughout life. The major drawback with DNA is that the patterning is done microscopically in a laboratory environment. Also, I feel there would be a problem of public acceptance of this technology since a cellular sample would be required. Since this technology was only discovered in 1980[33] it has not yet been automated for use in large database identification system. Therefore, this technology would not be practical in the driver licensing environment.

Automated Fingerprint technology was developed primarily for use in criminal identification to process and match fingerprint cards. These systems analyze the unique patterns of an individual's fingerprints. Since no two sets of fingerprints are alike, even for identical twins, this is a highly reliable technology. Automated fingerprints systems utilize a large database and employ both a verification and enrollment function which is desirable in the driver licensing identification system. Some disadvantages to this technology are that fingerprints can

be disfigured accidentally or purposely, and that inked fingerprints are often difficult to read.[34] In spite of these disadvantages, automated fingerprint systems would meet the needs of driver license identification in most instances. These systems are fairly user friendly and much study has gone into their applicability in the driver licensing environment.

Retinal scanning technologies measure the retinal blood vessel pattern of each eye. This pattern is unique and unalterable except in cases of injury or disease. Retina technology was developed as an identity verification system but has been adapted to also perform enrollment functions. The advantages of retinal scanning are that it has no law enforcement connotations and it is user friendly. The disadvantages are that retina technology has never been utilized with large databases, there is no way of determining that the applicant is submitting an adequate sample, and it lacks wide acceptance as a biometric identification technology.[35] In spite of these considerations there is good reason to believe retinal scanning would meet the identification needs of driver licensing.

## CHAPTER 4

## Biometric Technologies in the Driver License Environment

An examination of the validity of biometric identification in the driver licensing environment was explored in 1987 by the Federal Highway administration. Through this study it was determined that the most suitable technologies for the driver licensing environment were the automated fingerprint and retinal scanning systems. The problem was that neither of these systems had been utilized in environments similar to driver licensing.[36] Factors considered in this study were related to the impact on the normal operations of driver license offices which include:

- system accuracy.
- data capture time.
- reliability of data capture device.
- skill and effort required to operate the equipment.
- public acceptance of the technologies.
- central system response time.
- cost.
- implementation procedures.[37]

The results of this study will be covered in depth in another section of the writing. However, there are two other important factors to consider in biometric identification. These are the social and legal implications of biometric sampling and record keeping.

**Social Issues**

Any biometric identification system must have a high degree of acceptance and be user friendly if it is to receive a warm public reception. The public must feel the state is providing a necessary service for their overall good without an ominous sense of Orwellian public policy implications.[38] This was echoed by the American Civil Liberties Union which stated that biometric identification must be limited only to security purposes.[39]

Public response to biometric identification has been overwhelmingly positive. The American Trucking Association stated that a licensing system without a positive identifier was built on quicksand. They further stated:

> "It does not make sense to have an information system that could be tampered with. You need something at the heart of the system that cannot be falsified."[40]

Furthermore, in the Bryan, Texas, pilot project on retina scanning, conducted by the Texas Department of Public Safety over ninety-nine percent of the respondents to a public survey stated that the extra time required to process biometric data was justified to prevent fraud.[41]

The data collected in response to the public acceptance survey related to the American Association of Motor Vehicle Administrator's (AAMVA) Biometric Identifier Project, which was conducted in 1987 in the states of California, Texas, Illinois, and North Carolina, dispelled the myth that people connect fingerprinting with criminal activity. This project tested public acceptance of three biometric sample collection methods:[42]

- Retina scanning.
- Rolled fingerprints.
- Live scan fingerprints.

Of these technologies the retina scan was most refused by the public and live fingerprint scan was the most accepted.

The response percentages given on the biometric sampling questionnaires are as follows:

TABLE 1 [43]

| | LIVE SCAN | ROLLED SCAN | RETINAL PRINT |
|---|---|---|---|
| It is interesting | 84.0% | 73.7% | 80.5% |
| It takes too long | 13.1% | 9.1% | 14.4% |
| It is comfortable | 87.7% | 82.9% | 66.3% |
| It is safe | 92.2% | 88.6% | 82.5% |

| | | | |
|---|---|---|---|
| It is important | 81.8% | 79.7% | 67.4% |
| It is a good idea | 87.3% | 84.2% | 75.3% |
| It is scary | 5.2% | 7.3% | 8.3% |
| It is too messy | 7.1% | 8.6% | 6.8% |
| It is too hard to do | 4.9% | 6.8% | 7.4% |
| It invades your privacy | 7.8% | 11.4% | 12.9% |
| It is threatening | 5.2% | 6.5% | 8.0% |

It is notable that the live fingerprint scan received higher positive responses and lower negative results than the rolled fingerprint or retina scan technologies. However both fingerprint methods received a higher public approval rating than the retina scan.[44]

Further information obtained from the questionnaire demonstrated that ninety-eight percent of the participants felt the fingerprint technologies were acceptable, while ninety-seven percent felt the retina scan was an acceptable way to obtain a biometric sample. Another factor worth bearing out was that ninety-five percent of the respondents felt it was acceptable to utilize biometric identifiers to ensure the identity of persons issued driver licenses.[45]

Trends extrapolated from this survey were that participants in the survey group were more educated than the general population. However, as the education level increased there was greater resistance to all biometric technologies. On the contrary, persons with lower education and income levels were more positive in their responses to the biometric systems. A possible reason for this

particular trend was that the majority of responding nonparticipants came from California where the average income and education level is higher than the other test areas.[46]

Respondents to the survey who refused to participate in the enrollment procedures indicated several reasons for their refusal. The following table contains the reasons given for nonparticipation which were submitted by nine percent or more of the respondents.

TABLE 2 [47]

| REASON | PERCENT |
|---|---|
| Not interested | 40.9% |
| Don't have the time | 28.4% |
| Don't trust the technology | 11.2% |
| Don't understand why you are doing this | 9.0% |
| Don't want anybody to have this information | 14.3% |
| Invades my privacy | 18.6% |
| It is none of your business | 9.7% |
| It is too personal | 9.4% |

It is ironic to observe that persons who refused to participate in the actual biometric sampling but filed a survey response stated "not interested" or "don't have the time" as their two leading reasons for not participating in the biometric sampling. However, it must also be noted that there is some distrust of the biometric technologies as was indicated by the other responses in this survey. This

distrust level however is not as high as it might appear when it is considered that only fifteen percent of those who refused to be sampled returned a survey response. Furthermore, it can be argued that the fifteen percent who responded to the survey are not representative of the general population and these people had strong enough opinions on this subject to complete a survey.[48]

In concluding the social implications of biometric identification the following assumptions can be drawn. Biometric systems must be user friendly and convenient, while the concept of biometric identification must be viewed as beneficial and nonintimidating.[49] Also it can be stated that most people support the use of biometric identification as a driver license document security procedure.

## Legal Issues

The legal issues associated with any biometric identification system include:

- Fourth Amendment search and seizure issues.
- Fifth Amendment self incrimination issues.
- Recognition of the biometric sample as a unique identifier.

- Storage and use of biometric files.
- Legality of requiring the submission of the biometric sample.

The Fourth Amendment right against unreasonable search and seizure has been determined not to be applicable to fingerprinting for identification purposes.[50] Also excluded from Fourth Amendment protection were other identifying characteristics of which hand writing and voice were specifically noted.[51] In light of these general exclusions it would logically infer that retinal scanning identification procedures should also be excluded from Fourth Amendment protection.

Retinal scanning has one unique problem which does not affect the fingerprinting systems. Retinal scanning requires a search below the body surface. However, the reasonableness and legitimacy of the search should allow the use of retinal scanning. Reasonableness is determined by the degree of indignity caused by the search. This is measured by three factors. The first factor is the level of suspicion requiring the search. The second is the degree of physical contact between the searcher and the person searched, and finally the exposure of intimate body parts during the search. The only problem retinal scanning would have in the reasonableness test would be a degree of suspicion. Based on the fact that other searches which are

more intrusive than retinal scanning have been upheld as reasonable, there should be no problem with retinal scanning as an identification tool.[52]

The legitimacy of government obtaining and storing retinal scan data should be recognized because the state is acting within its valid interest to require identification. Therefore, the relatively minor intrusion of retinal scanning should be allowed since courts have upheld greater intrusions into driver privacy in the context of driver identification.[53]

Fifth Amendment considerations in the area of biometric data have been well documented in the fingerprint context. The courts have repeatedly held that fingerprints taken for identification purposes are not testimonial and are not included under Fifth Amendment protections.[54,55,56] The courts have further held that other identifying characteristics such as handwriting and vocal transmissions are not covered under Fifth Amendment protections.[57]

Another issue associated with biometric technologies is their recognition as a unique identifier. The only biometric identifier specifically recognized by the courts is the fingerprint.[58] The fingerprint has been so well

recognized that courts have required fingerprinting of a defendant during trial to verify his identity.[59,60,61]

Other biometric technologies are not as well recognized but have been granted credibility by decisions which have been rendered. The courts have held that retina scanning was legal for access to secured areas. This would infer that retina scan technology has identificatory credibility with the courts.[62] Another decision mentioned earlier lent credibility to handwriting and voice identification systems even though they were not explicitly recognized as biometric identifiers.[63]

The procurement, storage, and use of biometric identification files should be considered a legitimate government function. These files would be used to identify drivers and protect the public from fraud. This practice was upheld by the courts when they allowed the inclusion of fingerprints in non-criminal files.[64] This would infer that inclusion of retinal scans would also be allowed.

The final legal consideration is the state's ability to require the submission of biometric samples. The State of Texas currently requires the thumb or index fingerprints of all original applicants for a driver license or identification card.[65] However, the existing legislation does not require applicants to submit subsequent samples at

the State's request. Furthermore, a retinal scan sample is not currently required by law and could only be obtained voluntarily at this time.

In order to implement a comprehensive system of biometric identification in Texas the current legislation must be amended to require the submission of thumb or fingerprint samples at each phase of driver license issuance. If a retina scanning system were implemented, new legislation would be required to obtain retinal scans at each stage of driver license issuance process.

In concluding the legal issues it can be stated that there should be no significant legal problems in implementing a biometric identification system in the State of Texas.

# CHAPTER 5

# BIOMETRIC TECHNOLOGY EVALUATION

The evaluation of data will cover the retina scanning technology and the automated fingerprint (AFIS) systems. The AFIS technology will cover both the live scan and rolled print sample capture methods.

## Retinal Scan Method and System Analysis

The retinal scan is obtained by the applicant visually focusing on a particular location in a scanning instrument. The instrument scans a circular area of the retina with a low level infra-red light beam in a four-hundred and fifty degree circular scan and then records the light reflection level of the scan in a waveform. This waveform has a flat "x" axis and the intensity of the light reflected from the lighter tissue is recorded above the "x" axis, while the amount of the light absorbed by the blood vessels is recorded below the "x" axis. This waveform is then

digitized by the values of the peaks and valleys of the waveform. This digitized code represents the retinal pattern and is stored as the biometric identifier.[66]

Below are two sets of waveforms which have been overlaid for comparison. The first set matches while the second set does not. Alongside of the waveforms are the digitized codes for each individual scan.

[67]

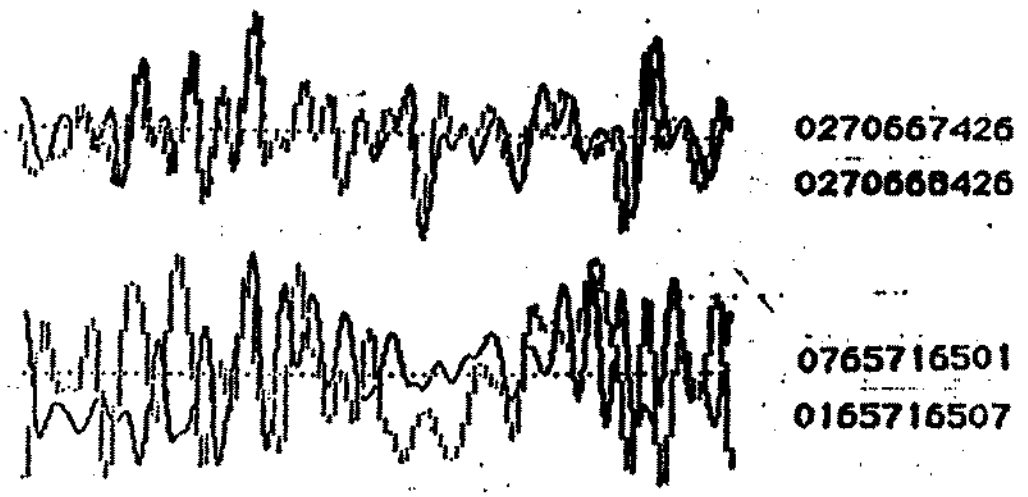


Fig. 1 Retina Scan Waveforms with corresponding digitized codes.

Retina scanning technology has proven highly reliable in identification verification processes but has left much to be desired in the enrollment processes. The following are the results of the retina scanning accuracy tests.

TABLE 3

| TEST | ACCURACY |
|---|---|
| Enrollment: | |
| • Unknown subject -- no duplicate in the database | 94.68% |
| • Unknown subject -- duplicate in the database | 61.71% |
| Verification: | |
| • Known Subject -- known record in database | 100.00% |
| • Known Subject -- unknown duplicate in database | 75.43% |

Data processing response time of retina scanning records is very fast overall. The following table reflects the response times related to the four tests in the previous table.



TABLE 4

| TEST | TIME |
|---|---|
| Enrollment: | |
| • Unknown subject -- no duplicate in the database | 2.09 seconds |
| • Unknown subject -- duplicate in the database | 2.36 seconds |
| Verification: | |
| • Known subject -- known record in the database | .94 seconds |
| • Known subject -- unknown duplicate in the database | .74 seconds |

Though the data processing time is remarkably fast for the retina scanning technology, it is offset by the time required to capture an adequate retinal scan sample. It takes an average of fifty-four seconds to explain the scanning process to the applicant. Added to this is an additional sixty-nine seconds to make the scan. This timeframe is expanded when dealing with applicants who are unable to understand instructions or who are trying to

fool the system. Furthermore, during this test period almost six percent of attempts to obtain an applicant retina scan were terminated due to the applicant's inability to understand instructions, inability to perform the operation of the instrument, or lack of cooperation.[70]

Another factor to consider in obtaining a retinal sample is that there is no method of determining if the sample given is adequate for identification purposes.[71] This problem resulted in a high percentage of poor quality images in the database during the test period which suggests that data collection problems were significant in the retina scanning technology [72]

Retina sample collection problems which were reported by the equipment operators primarily concern the retina scanning instrument. The operators suggested that a height adjustment, a head placement device, and a dual eyepiece would make data capture time and quality image procurement improve. They also noted that operator training in the retina scanning procedure and the personal computer associated with the retina scanning instrument were essential to obtaining acceptable retina samples. The operators further stated that persons with eyeglasses and eye problems had greater difficulty providing retina

samples. Another comment was that more intelligent people had less difficulty with the retina scanning device.[73]

A final factor to consider in the retina scanning technology is the capacity of the computer system required to store the biometric record. This system requirement would be relatively small since the enrollment scan of two eyes only requires one-hundred and forty-four computer memory bytes. Furthermore, only forty bytes are required for verification of a retinal pattern.[74] These relatively small records allow greater utilization of computer system capability which should be cost effective.

In conclusion, it must be reiterated that retina scanning technology was designed for access control. Hence, it is normally utilized with subjects who want to be identified and who are familiar with giving high quality enrollment and verification samples.[75] Therefore, implementation of retina scanning technology in a driver licensing environment is tantamount to requiring a technology to perform in a role for which it was not designed.

**Automated Fingerprint Method and System Analysis**

The fingerprint sample can be obtained in a number of ways which will be discussed later. However, once the sample is obtained it is classified into one of the Henry fingerprint classification groups[76] which are as follows:

- Whorl - fingerprints with at least one ridge that makes a circular shape around the center.[77]
- Plain Arch - fingerprints whose ridges enter on one side of the print and tend to flow out the other side.[78]
- Tented Arch - fingerprints whose ridges flow like an arch but have an upward thrust in the center.[79]
- Ulnar Loop - fingerprints whose ridges flow in a loop pattern toward the little finger.[80]
- Radial Loop - fingerprints whose ridges flow in a loop pattern toward the thumb.[81]
- Unknown/Scar - fingerprints which are damaged, scarred or do not fit into any other category.[82]

The fingerprints are then further classified as either left or right hand impressions. Next, the particular ridge endings or splits, called minutiae, are plotted by relative location on an "x" - "y" grid and reduced to a digital image[83] by their numerical location on the grid. An example of the minutiae and the plotting of them on the grid are shown below.

# FINGERPRINT MINUTIAE

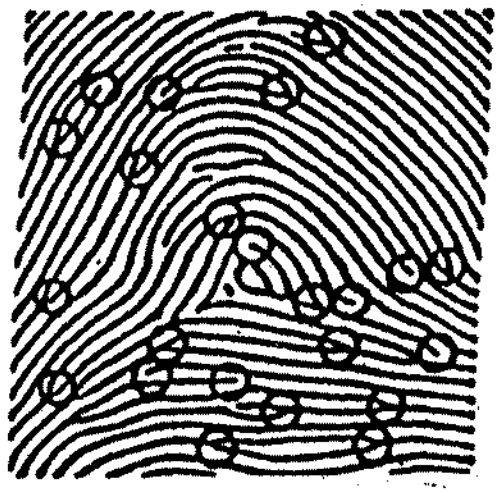

Fig. 2 Fingerprint with minutiae marked.

85

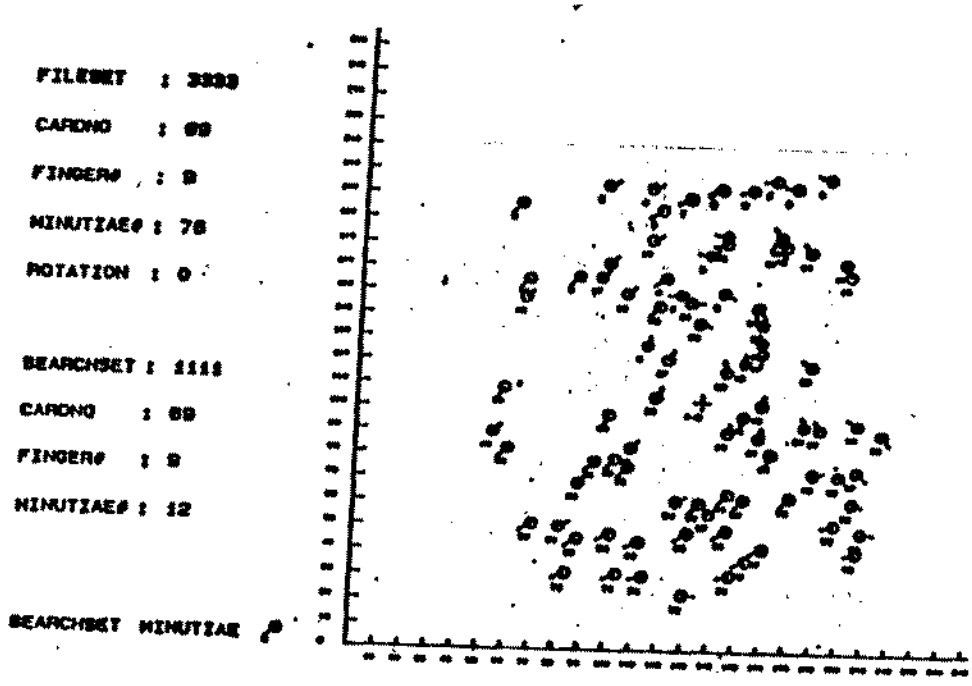


Fig. 3 Minutiae plotted a graph for comparison.

The digital image is then stored on a magnetic disk for comparison with other digital image records. AFIS database comparisons are made on the digital image level. The print image is reduced to the smallest size in which the minutiae are still discernable and stored on optical disks for reference purposes. This process, called compression, allows print images to be reduced in size for storage purposes without the loss of minutiae. The compressed image can be retrieved on a computer screen or printed for further manual identification verification.[86]

Fingerprint samples are obtainable through a variety of methods. However, for the purposes of the AFIS technology either inked fingerprint cards, inkless fingerprint cards or live scan readers are utilized.

The inked fingerprint cards were not utilized in the feasibility study because they are messy and difficult to obtain good quality prints from.[87]

The inkless rolled fingerprint card was utilized in the pilot test. This method was chosen because it was clean and did not have the law enforcement connotations associated with the inked print. Once the prints were obtained they were scanned by an optical reader which classified and processed the print images in the manner previously

noted.[88] To assure that a good fingerprint sample was obtained two sets of prints were taken from each applicant.[89]

The live scan fingerprint reader simply performs all the processing functions without any manual manipulation. The benefits of the live scan are its ease of operation, that it is not intrusive to the applicant, the computer makes the match, and no fingerprint knowledge is necessary for the operator. The scanner takes several readings to establish a record file and then performs a verification check on the record it has established.[90]

AFIS systems proved highly reliable in the verification process and performed much better than the retina scanning technology in all of the accuracy tests. The following table shows the results of the accuracy tests conducted on the AFIS technology.

TABLE 5 [91]

| TEST | ACCURACY |
|---|---|
| Enrollment: | |
| • Unknown subject - no duplicate in the database | 97.19% |
| • Unknown subject - duplicate in the database | 87.9% |
| Verification: | |
| • Known subject - known record in database | 100.00% |
| • Known subject - unknown duplicate in database | 90.98% |

The data processing time for the AFIS technology was not as fast as the retina scanning systems. However, the following table shows the response times of the AFIS technologies which were tested. The time for each technology is listed separately for comparative purposes.

TABLE 6 92

| TEST | LIVE SCAN | ROLLED PRINT |
|---|---|---|
| Enrollment: | | |
| • Unknown subject - no duplicate in the database | 71.29sec | 64.86sec |
| • Unknown subject - duplicate in the database | 74.38sec | 74.41sec |
| Verification: | | |
| • Known subject - known record in the database | 34.50sec | 49.43sec |
| • Known subject - unknown record in the database | 36.50sec | 44.26sec |

The data processing response time, though not as fast as the retina scanning process, fell within a reasonable timeframe. However, the total applicant processing time for the two AFIS technologies varied greatly. The live scanning process took only fifteen seconds to explain to the applicant, but took an additional two minutes and twenty seconds to obtain fingerprint samples. On the other hand, the rolled print technology took twenty-nine seconds to explain to the applicant, but only forty-four seconds to obtain the fingerprint samples. Furthermore, there was

very little the applicant could do to tamper with the fingerprinting process, consequently there was little problem in obtaining good samples. However, the live scan unit terminated just under two percent of the applicant samples and the operating personnel terminated over three percent of the rolled print attempts due to the applicant's inability to give an adequate fingerprint sample.[93]

The ability to verify that a quality fingerprint sample has been obtained is essential in the AFIS systems. To accomplish this the live scanner will not establish an applicant record until a good sample has been obtained and verified by the scanning unit.[94] On the other hand, the quality of the rolled print sample can be verified by the employee at the time the fingerprints are obtained. This single ability of the AFIS systems make them superior to the retina scanning systems in the driver licensing environment.

The operators using the AFIS system equipment rated the live scan devices as the easiest to operate and instruct the applicants to operate. They rated the rolled print as the second easiest to operate overall with the retina scanning systems as the most difficult to operate and explain to the applicant. The only negative responses by the operators concerning the AFIS systems were that more training time was needed for the live scan operators and that rolled prints

were difficult to obtain from persons with arthritis or dexterity problems.[95]

The most glaring problem with AFIS systems is the size of the data record. A fingerprint record for a set of two fingerprints in an AFIS database requires 297,320 data bytes.[96] Thus the capacity for a fourteen million driver record database would require a computer system capacity in excess of 4.17 trillion bytes and would require a minimum of one hundred matching units.[97] Such a system would be much more costly than a retina scanning system by virtue of the number of processors and database capacity requirements.

## CHAPTER 6

## AUTOMATED FINGERPRINT / RETINA SCAN ANALYSIS

Through the analysis of public acceptance, operator response, and system capability, it is feasible to implement a biometric identification system into the driver licensing process at this time.

The public responded favorably to biometric identification with a ninety-six percent favorable response to the AFIS systems and a ninety-three percent positive response to the retinal scanning system. Most persons polled felt that biometric identification was justified to prevent persons from obtaining multiple licenses. Additionally seventy-five to eighty percent of the persons polled thought biometric sampling was interesting, comfortable, safe, important, and easy to do. Persons contributing negative responses indicated that either they were not interested or did not have the time to participate in biometric sampling. It is interesting to note that no negative responses were critical of the biometric technologies. In conclusion, it must be stated that public response to biometric identification was overwhelmingly positive in regard to the technologies which were tested.[98]

The operators of the biometric technologies reacted favorably to all three technologies which were tested. They stated that all the systems were easy to learn to use and operate.[99] However, in a ranking scheme the live scan AFIS system was rated the highest by the operators, followed by the rolled print AFIS system and the retina scan systems respectively.[100]

In analysis of system capability, factors of system accuracy, data sample collection time, data collection performance, system reliability, and central system response time were considered.

System accuracy was dependant upon the capture of high quality biometric samples. Once samples were obtained the most accurate technology was the AFIS system.

The recognition rate of the AFIS for a duplicated enrollment record was ninety-two percent while the retina scan rate was only sixty-nine percent. Furthermore, the AFIS recognition rate for a false verification was ninety-two percent while the retina scan rate was only eighty-four percent. Other tests which enrolled new applicants who were not in the database showed the AFIS to have a nominally better accuracy rate of ninety-eight percent compared to the retina scan rate of ninety-six percent. Both AFIS and

retina scan technologies had a one hundred percent recognition rate for verification to a matched record in the database.[101] Overall AFIS had significantly better accuracy results on all the tests. However, in the critical test process to prevent multiple issuances of driver licenses the AFIS technology was superior.

The biometric sample collection times were averaged to determine which technology would create the least interference with the daily operations of the driver license office procedures. The AFIS rolled print technology took only one minute and thirteen seconds to obtain a quality sample. However, it must be remembered that over three percent of the rolled print sample attempts were terminated. The retina scan took just over two minutes to obtain a sample but terminated just under six percent of the sample attempts. Finally, the live scan fingerprint reader took the longest time to obtain a sample. It took just over two and one-half minutes to obtain adequate samples and only terminated just under two percent of the attempted readings.[102] In evaluating the capture times, it appears that both AFIS systems are better suited to the driver licensing environment than the retina system. The most important factor considered in sampling and collection times is the percentage of terminated sample attempts. These terminated attempts would adversely affect the public

acceptance of these technologies and would defeat the purpose of the biometric identification system which is to capture and record a unique identifier for each licensee in the State of Texas.

The reliability of the technologies is concerned with the system operational reliability. The test data is not conclusive in this area, however, the AFIS systems currently utilize alternative back up procedures which have been tried and tested. In the event of a breakdown of a single component existing back up procedures are activated automatically. The retina scan system has not been tested in this area due to the fact that the retina scan has never been utilized with a large database.[103] Hence, the AFIS technology seems to be better prepared to remain functional in the event of a single component breakdown.

The central system response time for the retina scan was significantly faster than the AFIS. However, the AFIS system did not exceed one and one-quarter minutes for enrollment of new applicants nor did it exceed fifty seconds for verification responses.[104] These response times for the AFIS are acceptable to meet the goal of implementing a biometric identification system into the driver licensing system.

# CHAPTER 7

## CONCLUSIONS

In closing, it appears that biometric technology is the best solution to curb driver license document fraud. The data indicates that the AFIS technology best suits the needs of the driver license environment to accomplish the goal of obtaining a biometric identifier on each licensed driver in the State of Texas.

The cost of a biometric identification system must be weighed against its potential benefit. A complete retinal scanning system with a 5 million record capacity was bid in 1990 at 4.3 million dollars. A comparable AFIS system for criminal record classification was designed and bid to the State of Texas at 14.3 million dollars.[105] A full AFIS system which would perform identification functions for 14 million driver records is estimated to cost around 30 million dollars.[106] This cost is minimal when it is realized that it amounts to less than ten percent of the financial losses directly attributable to driver license document fraud in Harris County, Texas, in 1986 alone.[107]

Thus, biometric technology appears to be the best option available to curb all types of crime by assuring that persons have only one driver license. This is true because the driver license document is utilized and recognized as positive identification in all areas of society.

ENDNOTES

1. Sinclair, Tom, Dunlop Farren, Mike Lawrence, Retina Scanning System Proposal, (Houston Security Time and Control Corporation,1987), 1
2. Federal Immigration and Naturalization Service, California Department of Motor Vehicles, Identification Update and Vision for Tomorrow, (1989) 3
3. Ibid., 5.
4. Milner, Joe E., Texas Department of Public Safety: Interoffice Memorandum: Xerox Copies of Birth Certificates, (1989)
5. Texas Department of Public Safety, Summary of DWI Involved Accidents in the State of Texas for Calendar Year 1989, (1990), 2
6. Texas Department of Public Safety, Summary of DWI Involved Accidents in the State of Texas for Calendar Year 1990, (1991), 2
7. Ward,Bernie,"Retinal Scanning Process", Sky, January 1990, 73
8. Wilson,Tom, "Biometric Identification Halts Fraudulent Entitlements and Duplicate Licenses", Government Technology, September 1990, 24
9. Sinclair, Retinal Scanning Proposal, 1
10. Federal Immigration, Identification Update, 2
11. Wilson, Government Technology, 44
12. Federal Immigration, Identification Update, 5
13. Webster's Seventh New Collegiate Dictionary,(Chicago, Rand McNally Co., 1967), 85
14. State of California Department of Motor Vehicles, Personal Identifier Project Feasibility Study Report, (1988), 2
15. Ward, Sky, 74
16. Ibid., 73.
17. Ward, Sky, 74
18. Wenchel, Functional Description, I-5
19. Ibid., vii
20. Ibid., vii
21. "Hi-tech License Index", Heavy Duty Trucking, (October 1988) 156
22. Hof, Business Week, 109
23. Wenchel, Functional Description, III-4
24. Ibid., III-1
25. Ward, Sky, 74
26. Hof, Business Week, 109
27. Wenchel, Functional Description, vii
28. Ward, Sky, 74
29. Wenchel, Functional Description, vii
30. Orkand Corporation, "Personal Identifier Project" Final Technical Report, (1990) I-2
31. Wenchel, Functional Description, vii

32. Ibid., III-4
33. Kirby Lorne T., DNA Fingerprinting, An Introduction (New York, Stockton Press, 1990) iv - 1
34. Wenchel, Functional Description, III-12 - 19
35. Ibid., III-10
36. Orkand Corp., "Personal Identifier Project", I-1
37. Ibid., IV-1
38. "FHWA Biometrics Study Draws Fire" Heavy Duty Trucking (September 1989), 36
39. Hof, Sky, 112
40. "Hi-tech License Index", Heavy Duty Trucking, 156
41. Texas Department of Public Safety, Retina Scan Pilot Project Final Report, (5 June 1987), 14
42. Orkand Corp., "Personal Identifier Project", IV-D-1 - 2
43. Ibid., IV-D-9
44. Ibid., IV-D-9
45. Ibid., IV-D-12
46. Ibid., IV-D-5
47. Ibid., IV-D-15
48. Ibid., IV-D-17
49. Ward, Sky, 82
50. Byrd v. State, 495 S.W. 2d 226 (1973)
51. U.S. v. Waller, 581 F. 2d 585 (1978)
52. Lindsay, Hart, Niel and Wiegler, to Eyedentify Inc., (1 July 1987), 7
53. Ibid., 5
54. Tea v. State, 453 S.W. 2d 179 (1970)
55. Aguilar v. State, 478 S.W. 2d 948 (1972)
56. Stanley v. State, 490 S.W. 2d 828 (1970)
57. U.S. v. Waller, 581 F. 2d 585 (1978)
58. Stevenson v. State, 380 F. 2d 590 (1967)
59. Burnden v. State, 211 S.W. 2d 197 (1948)
60. Byrd v. State
61. Cassell v. State, 507 S.W. 2d 853 (1974)
62. McMorris v. Alioto, 567 F. 2d 897 (1978)
63. U.S. v. Waller
64. Menard v. Saxbe, 498 F. 2d 1017 (1974)
65. Texas Traffic Laws, Driver's License Article 6687b Section 6(b)
66. Wenchel, Functional Description, III-5
67. Orkand Corp., "Personal Identifier Project", III-19
68. Ibid., IV-A-5
69. Ibid., IV-F-3
70. Ibid., IV-A-23 - IV-C-21
71. Wenchel, Functional Description, II-7
72. Orkand Corp., "Personal Identifier Project", IV-A-20
73. Ibid., IV-C-19
74. Wenchel, Functional Description, III-11
75. Orkand Corp., "Personal Identifier Project",IV-C-6
76. Ibid., II-2
77. Horgan John J., Criminal Investigation: Second Edition, (New York, McGraw Hill,1979) 113-114
78. Ibid., 113

79. Ibid., 113
80. Ibid., 113
81. Ibid., 113
82. Ibid., 115
83. Orkand Corp., "Personal Identifier Project", II-2
84. Fingermatrix Incorporated, Fingermatrix Fingerprint Identification Technology (An Overview), (New York 1988),II-8
85. Ibid., II-9
86. Orkand Corp., "Personal Identifier Project", II-3
87. Wenchel, Functional Description, III-19
88. Orkand Corp., "Personal Identifier Project", II-7
89. California Deaprtment of Motor Vehicles, "Personal Identifier Project "California Data Collection 1-Retina Scan 2-Inkless Rolled Fingerprint 3-Live Fingerprint Scanning"", (California Department of Motor Vehicles: 1989) videocassette
90. North American Morpho Systems, The Morpho-AFIS Solution to Document Fraud, (Morpho Inc., 1989) videocassette
91. Orkand Corp., "Personal Identifier Project", IV-A-5
92. Ibid., IV-F-3
93. Ibid., IV-B-7 - IV-C-21
94. North American Morpho, The Morpho-AFIS Solution vidoecassette
95. Orkand Corp., "Personal Identifier Project", IV-C-19
96. Ibid., III-4
97. Mr. Brian Withrow, Interviewed by author, notes taken Austin, Texas 5 march 1991.
98. Orkand Corp., "Personal Identifier Project", VI-3
99. Ibid., VI-3
100. Ibid., IV-C-19
101. Ibid , VI-1
102. Ibid., VI-2
103. Ibid., VI-4
104. Ibid., IV-F-3
105. Ibid., IV-G-3
106. Withrow Interview
107. Sinclair, Retina Scanning System Proposal, 1

## WORKS CITED

California Department of Motor Vehicles, "Personal Identifier Project "California Data Collection 1-Retina Scan-2 Inkless Rolled Fingerprint 3-Live Scan Fingerprint"", produced by the California Department of Motor Vehicles, 8 min., 1989, videocassette

Federal Immigration and Naturalization Service, California Department of Motor Vehicles, Identification Update and Vision for Tomorrow, January 1989

"FWHA Biometrics Study Draws Fire", Heavy Duty Trucking,September 1989,36

Fingermatrix Incorporated, Fingermatrix Fingerprint Identification Technlogy (An Overview), North White Plains, NY, 1988

"Hi-tech License Index", Heavy Duty Trucking, October 1988, 154-158

Hof, Robert D., "Forget the I.D. - Let's See Your Eyeball", Business Week, 20 November 1988, 109,112

Horgan John J., Criminal Investigation, Second Edition, McGraw Hill, New York, NY, 1979

Kirby, Lorne T., DNA Fingerprinting, An Introduction, Stockton Press, New York, NY, 1990

Lindsay, Hart, Niel, and Wiegler, to Eyedentify Inc., 1 July 1987, Transcript in the Biometric Identifier Project File of the Inspection and Planning Bureau of the Texas Department of Public Safety,Austin

Milner, Joe E., Texas Department of Public Safety Interoffice Memorandum, Xerox Copies of Birth Certificates, 5 March 1984

North American Morpho Systems, The Morpho-AFIS Solution to Document Fraud, produced by Morpho Inc.,9 min., 1989, videocassette

Orkand Corporation, California Personal Identifier Project Final Proposal, 1989, photocopied

Orkand Corporation, "Personal Identifier Project" Final Technical Report, 1990, photocopied

Sinclair, Tom, Dunlop Farren, Mike Lawrence, Retina Scanning System Proposal, (Houston Security Time and Control Corp.), June 1987

State of California Department of Motor Vehicles, Personal Identifier Project Feasibility Study Report, 6 December 1988

Texas Department of Public Safety, Retina Scan Pilot Project Final Report, 5 June 1987

Texas Department of Public Safety, Summary of DWI Involved Accidents in the State of Texas for Calendar Year 1989, 1990

Texas Department of Public Safety, Summary of DWI Involved Accidents in the State of Texas for Calendar Year 1990, 1991

Texas Traffic Laws, Driver's License, Article 6687b, Section 6(b)

Ward, Bernie, "Retinal Scanning Process", Sky, January 1990, 73-82

Webster's Seventh New Collegiate Dictionary, Rand McNally, Chicago,Ill., 1967

Wenchel, Liz, David Forsburg, Functional Description for a Unique Identification System for the Commercial Driver's License Information System, February 1988, FHWA-MC-88-048

Wilson, Tom, "Biometric Identification Systems Halt Fraudulent Entitlements and Duplicate Licenses", Government Technology, September 1990, 24,44

Withrow, Brian, Manger, Texas Department of Public Safety Automated Fingerprint Identification System, Interviewed by author, 5 March 1990, notes taken, Austin, Texas

## CASES CITED


Aguilar v. State, 478 S.W. 2d 948 (1972)

Burnden v. State, 211 S.W. 2d 197 (1948)

Byrd v. State, 495 S.W. 2d 226 (1973)

Cassell v. State, 507 S.W. 2d (1974)

McMorris v. Alioto, 567 F. 2d 897 (1978)

Menard v. Saxbe, 498 F. 2d 1017 (1974)

Stanley v. State, 490 S.W. 2d 828 (1970)

Stevenson v. U.S., 380 F 2d 590 (1967)

Tea v. State, 453 S.W. 2d 179 (1970)

U.S. v.Waller, 581 F. 2d 585 (1978)