

**FACIAL IDENTIFICATION TECHNOLOGY AND LAW
ENFORCEMENT**

JOURNAL ARTICLE

JO ANN WEST
VALLEJO POLICE DEPARTMENT

COMMAND COLLEGE CLASS XXII
PEACE OFFICER STANDARDS AND TRAINING
SACRAMENTO, CALIFORNIA

JULY 1996

22-0461

This Command College Independent Study Project is a FUTURES study of a particular emerging issue in law enforcement. Its purpose is NOT to predict the future but rather to project a number of possible scenarios for strategic planning consideration.

Defining the future differs from analyzing the past because the future has not yet happened. In this project, useful alternatives have been formulated systematically so that the planner can respond to a range of possible future environments.

Managing the future means influencing the future--creating it, constraining it, adapting to it. A futures study points the way.

The views and conclusions expressed in the Command College project are those of the author and are not necessarily those of the Commission on Peace Officer Standards and Training (POST).

INTRODUCTION

The potential for violence in America is almost everywhere. Each year, more than 23,000 people - nearly half the total number killed in the entire Vietnam War - are murdered. More than 170,000 are raped, and more than 6 million are victims of assaults. At least 13 million are victimized by property crimes, while about 1.5 million victims of violent crime are treated by our health care systems. The total economic cost of crime in this country - in a single year - comes to a staggering \$70 billion.¹

Each year we spend more than \$75 billion on the law enforcement and criminal justice systems, another \$50 billion on private security agencies, and untold amounts on often unsuccessful efforts to protect our homes and businesses.²

If we could reduce crime by only 1 percent, it would mean 230 fewer murders, more than 1,700 fewer rapes, 60,000 fewer assaults, and at least 130,000 fewer property crimes. It would mean 15,000 fewer victims of crime burdening our already hard-pressed health care systems, and it would mean a savings of at least \$700 million in economic costs-savings that would be realized each year.

While the problem of crime, especially violent crime has received significant national attention, there has been little discussion of the role that new technologies can play in addressing these problems. This is especially important as law enforcement agencies are faced with severe budget restrictions.

Although technology, in itself, will not solve the crime problem, new technologies can significantly increase the capabilities and efficiency of law enforcement operations. New technologies also can provide new options for law enforcement agencies seeking ways to reduce the use of violent or lethal force in confronting uncooperative suspects. Finally, new technologies are essential to assist law enforcement in simply maintaining some parity with the methods criminals employ trying to escape detection and avoid apprehension. While there may be limits to the amount of improvement technology is capable of producing in the levels of crime, the promise of productivity improvements offered by technology is clear.

From 1970 to 1991, crimes per police officer increased more than 65 percent, while only 45 percent of all violent crimes are cleared from the books each year. Because it is unlikely we can afford to double our expenditures on law enforcement, improving the productivity and effectiveness of policing is essential.³

It is evident that Americans are concerned about crime. As violence proliferates on city streets and in rural towns, society is seeking better ways to stop it. Adding more police officers to department rosters and implementing numerous social and economic programs constitute some of the current methods of addressing the crime problem.

Citizens are looking for methods to deter criminals through available technology that will limit their access and identify criminals. Businesses are investing more than ever in hiring guards and installing high-tech gizmos like tilt and zoom closed circuit cameras or magnetic card access

systems. The current outlay is more than \$22 billion each year, up 16 percent from 1990 according to Leading Edge reports, a research firm based in Cleveland, Ohio. By 1997, the expenditure is expected to soar another 35 percent to nearly \$31 billion.⁴

This emphasis on security has encouraged the development of electronic identification technologies which can be used to insure access security. There are a variety of people recognition technologies in existence. They include such types as fingerprints, DNA, voice recognition, retina scan, and hand geometry. Among the newest and most intriguing of these tools is facial recognition. This technology is making it possible for computers to digitize, analyze, and identify faces. This technology compares a real-time picture from a video camera to digital pictures in a computerized database and then identifies the subject. The possibilities for law enforcement are exciting. This technology not only has the potential to be used to provide access security, but it also it could be used to identify and apprehend criminals by analyzing surveillance photos.

ISSUE AND SUB-ISSUES

The issue this article will consider is facial identification technology and the potential impact it will have on law enforcement as a tool to curb crime. It focuses on a strategic plan to insure the research, development and implementation of facial identification as a tool for law enforcement in deterring crime and identifying criminals.

Three primary sub-issues arose when doing research on this issue. The first relates to the

establishment of a database. This is a key element to the success of the technology as it relates to law enforcement. It will be necessary to coordinate existing databases, such as the Department of Motor Vehicles and mug shot databases that are maintained at state and local levels. This will result in a meaningful and comprehensive database for the implementation of facial identification technology for law enforcement purposes.

A second sub-issue that was identified during this research was the potential impact that facial identification technology may have on a citizen's right to privacy. It is certain that civil libertarian groups will express concern that the use of video surveillance cameras in public settings could be abused as could a statewide or national database. There are likely to be concerns relating to the confidentiality of the database and rights to access the database.

A final sub-issue that arose during the research relates to the potential impact that facial identification technology may have on the workplace environment and operation. The desire for a safe and secure workplace has become an issue as a result of numerous incidents of workplace violence. Several court decisions have found employers liable for failing to provide a safe work environment. As identification technology becomes more advanced, employers may be found liable if they fail to implement the technology. The implementation of this technology may require changes in the operational procedures for most facilities. This may result in a more suspicious, less trustful workplace that is no longer easily accessible to workers, their families and their friends. There may be employee resistance to these changes in the work environment and a fear that the technology may be used to monitor performance rather than insure security.

HISTORY OF IDENTIFICATION SYSTEMS

Prior to discussing the research findings and recommendations, it is important for the reader to be familiar with the various people recognition technologies that are currently either in existence or in the development stage.

Before the development of fingerprinting, people identified some criminals and slaves by branding or tattooing them, or by amputating one of their limbs. Other early methods were less reliable though more humane. They included photography and the Bertillon system, a technique based on the measurements of the arms, legs, and other parts of the body.

The second century B.C., marked the first use of fingerprints for positive identification when Chinese rulers used their thumb prints to seal important documents. Those in government were able to recognize instantly the distinctive imprint of the various leaders and ensure the authenticity of information.⁵

Fingerprinting became a scientific method of identification in the 1880's with the research of Sir Francis Galton, a British anthropologist. Galton calculated mathematically that no two people could have exactly the same fingerprint patterns.

During the 1890's, two police officers, Juan Vucetich of Argentina and Sir Edward R. Henry of Great Britain, developed fingerprint classification systems. The Henry system became the basis of the fingerprint systems used in the United States and many other countries.

Today, society still recognizes that people's fingerprints hold undeniable, unchangeable evidence of their identity. However, the fingerprint identification process has naturally broadened to a much greater scale. While the eye is still an important part of fingerprint analysis, technological advances now allow electronic storage, searching, and matching of fingerprints. This automation has overwhelmingly improved criminal identification and arrest history verification by more than 50 percent in recent years. This technology is being expanded to other areas such as social services, drivers' licensing, gun control, and immigration.⁶

Fingerprint identification will continue to be a valuable tool in the identification and apprehension of criminals. However, fingerprints are not always available as a tool. Criminals often wear gloves, refrain from touching surfaces, or wipe their fingerprints from the crime scene. As a result, other methods of identification become important.

Another method of biometric identification is that of genetic profiling or DNA fingerprinting. Scientists contend that every human being other than an identical twin can be identified by his or her unique genetic code; DNA extracted from blood or other tissue at a crime scene can be compared with a suspect's genetic material. DNA profiling was first used in a United States court in 1987. It was hailed as the greatest advance since fingerprinting. Since that time, DNA identification has been used to link in excess of 700 individuals to crimes.⁷

Current biometric research is looking into innovative ways for machines to recognize human beings for identification purposes. Retina scanning is one method that reads the unique blood

vessel pattern in the retina of the eye and records it in a database. This system is being tested at the Avoyelles Parish Sheriff's Office in Marksville, Louisiana. The Automated Biometric Identification System went on-line in May, 1986 by Data Security Systems, Inc. of Bunkie, Louisiana. It is being used to confirm the identity of inmates who have prior bookings on file. The advantage to this system over fingerprinting is that it is faster and takes less storage space on a computer than fingerprints. Chances are one in a million of making a misidentification with one eye and one in a trillion if both eyes are scanned.⁸

One of the most promising biometric identification technologies emerging today is that of facial recognition. All people have unique facial signatures. Researchers envision using this technology to positively identify individuals, regardless of changes in their appearance. The potential uses are endless. When completed, it could be employed for any military, law, enforcement, or civilian use where personnel need to be identified. The advantages are tremendous. This technology distinguishes itself from other biometrics approaches because it is passive, not intrusive, light-independent, and invulnerable to disguises.

FACIAL IDENTIFICATION TECHNOLOGY

In Stanley Kubrick's late - 60's film *2001: A Space Odyssey*, a flight attendant of the future greets scientists at a space-station checkpoint. "Welcome to Voice Print Identification," she says congenially from a video monitor, inviting the scientists to "imprint" their voices against a computer's memory. Today, scenes such as this are no longer fictional, as a variety of people recognition technologies have come to fruition. Among the newest of these tools is facial

recognition. There are a variety of facial recognition methods being researched and are described below.

NEURAL NETWORK TECHNOLOGY

Neural technology teaches computers to recognize faces in much the same way that our brain recognizes faces. Our brain has what can be categorized as a “facebase”. It contains the faces of everyone we know. When we are out on the street, walking past a parade of people, we are comparing each passing face against the ones we’ve remembered. If we get a match, a bell goes off in our head and we instantly recall who that person is. This is essentially what neural network technology does.

There are several companies currently researching neural network technology as a means of face recognition. One company, Miros, Inc. of Wellesley, Massachusetts has released the first commercially available program that can recognize human faces with an accuracy greater than 99 percent using neural network technology.

Miros’ program, called TrueFace, relies on major new developments in neural-network processing. Neural-network software is designed to mimic the brain’s functionality. It can recognize subtle patterns in context. The advantage of neural networks as recognition tools is that they can also learn from their own experience, correcting and storing information based on prior mistakes.

The software works by recognizing differences in lightness and darkness that define a person's unique features, comparing the patterns of a just-snapped photo with those in a stored reference image. Differentiating faces is particularly difficult because of the wide variability of facial expressions and orientation, hair styles, the bobbing of eyebrows, and such artifacts as glasses or three day growth of beard. Neural network software differentiates constant facial features, such as the shape of the nose and mouth, while ignoring variable ones, such as changes of expression and hairstyle. The neural-network software looks at an image of a face as a set of pixels that have varying degrees of lightness and darkness. The software then evaluates the contrasts of lightness in number value. The TrueFace program requires a 486 or Pentium PC with 12 Mbytes of RAM, a black and white camera with a frame grabber and software interface, and image storage, either on a smart card or a database. In operation, the software compares two faces and returns a confidence level of how well the faces match in about a second.⁹

Photobook is another neural network facial recognition process that has been developed by Alex Pentland at the Massachusetts Institute of Technology. Photobook treats mug shots not as images per se, but as visual information. Thus, the computer never really "sees" someone's face. Instead, it interprets each picture as a grid of information, as defined by a branch of mathematics called information theory. An image of a face imparts a unique set of information to a viewer. This computer program analyzes the content of that information and compares it with the image database.

Photobook uses a two-tiered method to recognize faces - a holistic view and feature analysis. On

the holistic side, the computer gives a facial image a quick overview, ascertaining how the face fits together as a whole. Then, by treating the image as a matrix of information, it searches for eigenvectors, or mathematical patterns, characteristic of that particular face.

Photobook can verify individuals in less than 10 seconds with an accuracy of nearly 97 percent, falsely rejecting someone less than 2 percent of the time and falsely verifying someone less than once in 10,000 times. In contrast, computerized fingerprint scans showed no false verifications but falsely rejected people's identify 9 percent of the time. Verification systems using vocal patterns, handprints, or eye retinal patterns turned in slower and poorer results than the eigenface system.¹⁰

KEN PROJECT

The Institute for Scientific Computing Research at Lawrence Livermore National Laboratory is developing a real-time face recognition system entitled "KEN". KEN software represents faces as labeled graphs. Faces are stored as a face graph model in the database. The software then compares a photo from a video camera in real time to the face graphs in the database. KEN is currently capable of classifying a face in real time, from a database of 100 faces with a positive identification rate of up to 90 percent and less than a 1 percent false positive recognition rate.¹¹

FACIAL THERMOGRAPHY

Another method of facial identification being researched is that of facial thermography. Like a fingerprint, the pattern of blood vessels beneath a person's face is unique. First, an infrared

camera captures a portrait of a face. The image highlights areas, such as blood vessels, that display a higher temperature than the surrounding flesh. A computer compares the infrared portrait to one stored in a database. The program begins by matching general facial features and then moves on to the finer data points.¹²

LIVE VIDEO FACE RECOGNITION

One of the biggest problems in digital recognition is finding the face in an image. This is of particular consequence when dealing with live video camera monitors. How does the computer find a person's face among all the other visual objects in a video? Research is progressing in this area, also. A product called FACEit has been developed that recognizes faces in live video and compares them to faces contained in a database.¹³

APPLICATIONS IN LAW ENFORCEMENT

A woman walks into a police substation to meet with a detective. She was a victim of a robbery at the local convenience store. She says that she can identify the suspect and thinks she has seen him before. She expects to spend time looking through mug-shot books like those used on television police shows. Instead, the detective sits down in front of a computer work station, inserts the video surveillance tape of the robbery, and within seconds matches the photo on the surveillance tape to a mug shot in the database. This is just one of the potential applications of facial recognition technology.

The marketplace may find even more applications for face recognition technology. British

Telecommunications is researching a security system using the technology. It would use video cameras to scan crowds of shoppers and then match those faces against a database of mug shots of criminals who have repeatedly been caught shoplifting. If a match occurred, the system would alert security guards.¹⁴

Face recognition technology could be used to surveil secure areas. It could be designed to sound an alarm when the system sees a stranger. That face could then be stored in the database so that at any time, the user can scan through all the stranger images to see who has been caught. This could be used to keep an eye on the entrance to some area restricted to people not in the database.

In a surveillance mode, the system could keep track of the comings and goings of a familiar person or people in its database. So, for example, if the police wanted to monitor an individual leaving or entering a building, they could use it to record when and how often he/she was seen.

The United States Army, too, has been looking at this technology for itself, for other branches of the military and for federal law enforcement agencies. One is a simple secure-entry system.

Military personnel would have their faces stored in the system. Then, when someone was trying to gain entry to, say, a nuclear submarine, the face recognition software would check to see if that person was authorized to do so. If not, access would be denied.

This technology could be used to thwart terrorists and drug runners. The faces of known

terrorists and drug runners could be scanned into a database. Face recognition cameras around public locations could check whether certain known suspects were showing up frequently. As was alleged in the Oklahoma bombing case, the suspects typically scope out a building or other target many times before doing a job. This technology could alert federal agents of the existence of known terrorists at a particular locations. In addition, cameras at customs checkpoints could spot the faces of known drug dealers who typically use disguises, fake passports, and phony visas.

The Massachusetts Department of Motor Vehicles plans to test it on drivers who claim they've lost their licenses and want replacement. The goal would be to see if those drivers really are who they claim to be, thus foiling those trying to obtain phony identification. Fingerprints, of course, could also verify identities, but fingerprinting takes so much time that it is impractical to use on everyone. Since every driver's photo is already on file, scanning a face and matching it against a large set of "faceprints" would be easier.¹⁵

Another potential application for the utilization of facial identification technology would be to assist in locating missing children. Imagine if there were a national or international database that contained the photos of all children, taken from schools and day care centers. Photos of missing children could be compared against this database on a constant basis. This has the potential in resulting in the identification of thousands of missing children that are reported each year. It would certainly be more productive than any system that is currently being employed.

Automatic teller machines (ATM) are the source of annual fraud that in some estimates totals

millions of dollars per year in the United States. Siemens Nixdorf of Germany has developed an automatic teller machine that identifies users by their faces. When the user inserts his or her chipcard, a camera integrated in the ATM automatically takes a photograph of the user's face and compares facial features with the reference image stored on the card. In the future, it is possible that the card could be eliminated and the computer would rely solely on comparing your face to a master database. This would, also, be convenient in that you would not have to worry about losing your ATM card or forgetting your Personal Identification Number because you always have your face with you.¹⁶

Fraud in government benefits payments is estimated at tens of billions of dollars per year. The Connecticut state legislature passed a law requiring that AFDC and General Assistance recipients be biometrically imaged for identification purposes. While Connecticut is currently using fingerprint scanning as a means of biometric identification, facial recognition technology has the potential to be used in this arena to detect fraud. It would prevent people from receiving welfare benefits under more than one name or from receiving benefits improperly from more than one town or state program.

Fraudulent prescriptions could also be impacted by using this technology. Patients receiving prescriptions could have their face scanned into a master database. Then, doctors and pharmacists could track a patient's prescription history to insure that the patient is not receiving duplicate prescriptions from unknowing doctors, and, also, insure that the prescriptions are authentic. In addition, the pharmacist could verify the identity of the recipient.

The possible applications for facial identification technology in both the private and public sector are limitless. Once this technology is completed, it could be employed for any military, law enforcement, or civilian use where personnel need to be identified.

FACIAL IDENTIFICATION TECHNOLOGY AND PRIVACY INTERESTS

Law enforcement needs and privacy interests often clash. The use of technology by law enforcement is no exception. When the police in West Windsor, New Jersey arrested Mauro I. Donis last year, it was not because they observed Mr. Donis violating any law as he drove along U.S. Route 1, but because a patrol car computer scanner determined that he had a suspended driver's license. Now, the scanners have become the focus of a novel lawsuit in which Mr. Donis argues that the police singled him out arbitrarily, without reasonable suspicion or probable cause, and that the subsequent computer inquiry into his driving and criminal records amounted to an illegal search.

This case, which is winding its way through the Appellate Division of the New Jersey Superior Court, is the latest of a small but growing number of legal actions challenging police use of computer scanners or mobile computer terminals. It is yet another chapter in the larger debate over just how far high-tech policing can go without trampling over people's constitutional rights.

For law enforcement officials, they are new generation weapons in the war on crime that enable the police to better protect the public, even at the expense of a little privacy. But for civil libertarians, they conjure Orwellian images of Big Brother. In the case of facial recognition

technology, there will likely be the concern that the technology will be abused. Will cameras that recognize you eventually track you down and feed your itinerary into government and corporate databases? Technology proponents dismiss such concerns as far-fetched and based on the hypothetical rather than the practical. Regardless, the concern is there and must be dealt with if facial recognition technology is to reach its full potential in the law enforcement arena. If law enforcement is to take advantage of this technology, then it must address these privacy issues. Regulations must be in place to govern the use of the technology. Groups such as the American Civil Liberties Union must be involved in the development of the technology and its implementation.

Already, more and more video cameras are appearing in public places and people accept the trade-off of some privacy for their safety. At automatic teller machines, for example, the presence of video cameras make people feel more secure. The impact of video surveillance systems was studied in King's Lynn, Norfolk in Britain where a network of forty-five cameras was installed in a leisure center, car parks, an industrial estate and streets of a housing estate. Interviews with 96 percent of residents showed a positive attitude towards installation of the system. An independent study of the Police Research Group showed that 53 percent of respondents said the system made them feel safe, 62 percent thought it deterred crime, 74 percent thought it prevented crime and 80 percent welcomed installation in public places. Only about a third of the respondents thought negatively about the system.¹⁷

Used in the proper way, face recognition technology might foster a small-town environment

where you know the good from the bad. For the good people, doors open and services should be available to them just by showing their face. Privacy is not so much a question of technology, but one of preventing authorities from giving out information about where you go and what you do. As long as different companies and government agencies don't provide such information to a central source, some of the concerns should be alleviated.

A STRATEGIC PLAN FOR THE FUTURE

This research was designed to develop a plan through which law enforcement will best be able to insure the development and implementation of facial recognition technology to meet law enforcement needs. The process utilized involved extensive research, literature scanning, discussions and brainstorming with professionals whose backgrounds, training and education established that they had a professional connection to law enforcement and/or facial identification technology or who were potential stakeholders. Professionals who participated in the research included representatives from the California Department of Justice, California Department of Motor Vehicles Biometrics Division, the American Civil Liberties Union, California Occupational Safety and Health Association, Vallejo Visitor and Convention Bureau, municipal law enforcement, county law enforcement, and the media.

This research revealed several projected trends and events that were likely to occur in the future that would impact the successful development and implementation of facial identification technology in a law enforcement setting. The research indicates that there will be an increase in violent crime, particularly in the workplace, that will create an environment that encourages the

development and implementation of facial identification technology. At the same time, however, the research shows that citizens will be concerned that their privacy may be violated with the implementation of this technology. It was projected that this citizen concern will result in strict regulations for the utilization of this technology and the development of a secure network to prevent unauthorized use of the database. In addition, a critical component that was expressed by the law enforcement and technology professionals was the need to develop a standardized facial database to insure compatibility between law enforcement agencies and to expedite the development of a product that is usable by law enforcement.

This research, also, stresses the importance of law enforcement involvement in the research and development of the technology so that it meets the needs of law enforcement. Often, law enforcement is forced to try and modify existing technology instead of being a driving force in the development of a product that is designed to meet law enforcement's objectives.

To that end, a strategic plan must include the development of a partnership between private industry and law enforcement to insure the development of this technology. Also, law enforcement agencies must work together to facilitate the development of standardized databases that are accessible to all law enforcement agencies.

This research resulted in the development of a strategic plan to manage and realize the eventual development and implementation of facial identification technology in law enforcement. The researcher recommends the formation of a statewide task force to research and implement facial

identification technology as a method for reducing crime. The task force should comprise as participants those stakeholders that were identified in the research. The following five agencies are recommended as participants in the task force:

1. California Department of Justice
2. California Department of Motor Vehicles
3. United States Department of Defense
4. California Police Chief's Association
5. California Occupational Safety and Health Association

This strategy requires that the Department of Justice take the lead as a catalyst and project manager in forming the statewide task force. The Department of Justice has the clout to insure that the researchers have access to databases for the research and design of the technology and, also, have access to funding sources for the development and implementation of the project.

The Department of Justice provides law enforcement services for every law enforcement agency in California. They are the most likely coordinator for a statewide digitized photo database that can be accessed by all law enforcement agencies. In addition, they would have the ability to facilitate a national database.

The California Department of Motor Vehicles participation in the task force is important because they maintain the largest statewide digitized photo database in California. The Department of Motor Vehicles has a biometrics division which has expressed interest in cooperating with the development of facial identification technology during the research phase of this project. There are advantages for the Department of Motor Vehicles as well in that the technology has the

potential to be utilized to eliminate fraudulent driver's license applications and to aid in the collection of delinquent fees by identifying customers who owe fees instantly.

The Department of Defense is already committed to assisting law enforcement in identifying technologies that already exist for the national defense and transferring those technologies to law enforcement. This was formalized in a partnership that was formed between the United States Attorney General's Office, the United States Department of Justice, and the United States Department of Defense in 1993. To this end, the Department of Defense is already involved in the research and development of facial identification technology at the Lawrence Livermore Lab. It is their hope that this technology will be a valuable tool to law enforcement.¹⁸

The California Police Chief's Association is an organization that represents nearly every police chief in California. They have the ability to garner support from their members' local governments for the plan. This will insure participation and financial support for the task force. In addition, many of the members control facial databases on the local level through mug shot systems. It is important that they support a plan to standardize the digitizing process and be willing to support a statewide database that is accessible by all law enforcement.

The California Occupational Safety and Health Association is included in the task force because they are in the business of creating safe work environments. They are drafting standards of violence prevention for nearly every industry in the state. They will be supportive of facial identification technology as a tool to create a safe workplace.¹⁹

IMPLEMENTATION STRATEGIES

The ultimate goal of the task force is to insure the development and implementation of facial identification technology in law enforcement as a means of reducing crime. Their first task will be to raise public awareness of facial identification technology and its potential applications to law enforcement. The task force must sell it to the public as a viable tool to help reduce crime. The public's understanding of the technology and its potential applications should result in their support for this tool for law enforcement. It will then be difficult for the civil libertarians to convince politicians to oppose it if the public favors facial identification technology as a realistic method of deterring crime and identifying criminals. Extensive media coverage of the concept of facial identification technology, its benefits to law enforcement and the proposed task force will help educate the public on the concept and ultimately result in their support. In addition, timely press releases on the progress of the task force will maintain public awareness and will motivate the task force to continue in their efforts.

The first job of the task force will be to meet with researchers and identify their needs for further research and design. This must include the identification of a standardized format for digitizing photos. An additional task will be to identify potential funding sources. Once these needs have been identified, the task force must establish standardized formatting for the digitized photo database, develop a plan to integrate databases, determine specifications for facial identification technology, meet and present specifications to the researchers and secure funding sources. It is anticipated that this process will take approximately one year.

The goals of the task force in the second year will be to develop guidelines for use of the technology, meet with the American Civil Liberties Union to discuss their concerns, facilitate an agreement with a researcher to develop a facial identification product that meets law enforcement needs and draft and finalize an implementation plan.

Concerns by the public that facial identification technology could be abused were recognized early on in this research. It is hoped that these fears can be allayed by regular media coverage on the significance of facial identification technology as a law enforcement tool and by keeping the public informed of the task force's progress. In addition, regular meetings with labor union representatives to keep them informed of the task force's progress relating to implementation plans for the technology is very important. Labor unions will likely fear that this technology will negatively impact the work environment and may be used to monitor employee productivity. They need to be allowed to express their concerns to the task force and those concerns must be addressed by the task force.

A potential obstacle that was identified is the American Civil Liberties Union. Their concerns will relate to right to privacy issues. If they are not dealt with appropriately, they could create fear among the public and detract from the support of the program. Therefore, it will be necessary for the task force to consult regularly with the American Civil Liberties Union throughout this process. In addition, one member of the task force from the Department of Justice should be designated as the liaison with the American Civil Liberties Union with responsibility for keeping the rest of the task force informed of their position.

Integration of photo databases may not be easy to accomplish. There may be reluctance to standardize formats for the digitized database. The responsibility for completing those tasks is that of the Department of Justice, but should require approval of the Department of Motor Vehicles and the California Police Chief's Association because they control databases that are important to the project. The Department of Defense should work with these agencies to insure that the specifications that are developed are compatible with the development of the technology.

Another obstacle is the current adversity between local governments, county governments, and state government. All are competing with each other for funding and seeking to retain control of their resources. The inclusion of the California Police Chief's Association should be able to minimize that adversity by coming together for a purpose that is in everyone's best interest. In addition, varying levels of government are included in the task force with equal levels of input into the process.

This researcher would be remiss if fiscal concerns were not addressed in this plan. It is hoped that the inclusion of various agencies, particularly the Department of Justice and the Department of Defense, will foster funding for the implementation plan. The Department of Defense has been asked by the Attorney General's Office to develop technology that will assist law enforcement. Their involvement in the task force will hopefully increase the probability of federal funding for the project. In addition, the Department of Justice, Department of Motor Vehicles, and Occupational Safety and Health Association involvement may result in state funding. Widespread media coverage of the task force should result in the support of the business community which is

another potential resource for funding. Also, private developers of facial identification technology may view this project as a worthwhile investment due to the potential market for their product.

CONCLUSION

Implementing new ideas takes planning and that planning needs to anticipate the probable future. Without planning, it is difficult to take advantage of opportunities and deal with obstacles in an effective manner. It is apparent that facial identification technology will exist in the future. However, law enforcement now has an opportunity to be involved in its development. Planning for its eventual introduction will aid law enforcement when it is ready for implementation. In the past, law enforcement has allowed private industry to be the developer of technology. Law enforcement has been satisfied to ride on their coattails and are, therefore, left with a mediocre product that does not always meet the needs of law enforcement. Law enforcement needs to become a driving force in the research and development of technology so that its needs are satisfied.

Law enforcement should work with private industry in the research and development of facial identification technology. This will require budgeting for the research and development of the technology. Since budgets are often tight, planning becomes even more critical. Law enforcement needs to look ahead to the future to see what issues, trends, events will benefit from the technology. Then those groups should be targeted for financial assistance. For example, if facial identification technology were to be promoted as a tool for locating missing children, then special interest groups such as the Polly Klaas Foundation might consider giving financial support

to such a project.

The development of a facial database is critical to the successful research and implementation of this technology. At this time, there are several sources of databases for the technology, but there is little coordination between agencies that have control of these databases. Consideration must be given to government oversight of these databases to insure that they are compatible, use standardized formats, and are accessible to all law enforcement agencies.

Law enforcement needs to anticipate and plan for some of the negative implications that may result from the implementation of the technology. For example, one of the trends identified in this research was an increased concern about privacy rights. Law enforcement must be sensitive to that issue and put policies and procedures in place that would alleviate some of those fears. The inclusion of the organizations such as the American Civil Liberties Union, community activists, and elected officials in the development of regulations governing the utilization of the technology will benefit law enforcement's endeavor to utilize facial identification technology in the future.

There are no guarantees that the future we plan for will be the future that comes to pass. However, if we do not plan, then we will have no control over our future. Facial identification technology is definitely going to be a part of the future. The impact of the role it will play for law enforcement in the future is largely dependent upon our involvement in its research and development today.

ENDNOTES

1. International Association of Chief's of Police, Violent Crime in America, International Association of Chiefs of Police, 1993.
2. United States Department of Justice, Justice Expenditure and Employment, 1990, Bureau of Justice Statistics, U.S. Department of Justice.
3. International Association of Chief's of Police, Violent Crime in America, International Association of Chiefs of Police, 1993.
4. A. Toufexis, "Workers Who Fight Fire With Fire," Time, April 25, 1994, p.34.
5. NEC Technologies, Inc, "AFIS: A New Generation of Identification," Government Technology, August, 1994, p.25.
6. Ibid.
7. Shannon Brownlee, "Science Takes the Stand," U. S. News and World Report, July 11, 1994, p. 26.
8. Bill Clede, "Identification by Retina Pattern," CompuServe Library Article, 1989.
9. Arielle Emmett, "Coming Face to Face With the Future," Computer Graphics World, June, 1994, p24.
10. Richard Lipkin, "A Face By Any Other Name: How Computers Recognize Faces," Science News, April 2, 1994, p. 12..
11. University of California, Ken Project - Real-World Face Recognition, University of California, Lawrence Livermore National Laboratory, 1994..
12. Hearst Corporation, Faceprint Security, Hearst Corporation, 1995.
13. Joseph Atick, "Face Recognition from Live Video for Real-World Applications-Now," CompuServe Library Article, April, 1996.
14. Evan I. Schwartz, "A Face of One's Own," Discover, December, 1995, p. 78.
15. Ibid.
16. Siemens Nixdorf, Automatic Teller Machines from Siemnts Nixdorf, Siemens Nixdorf Informationssysteme AG, January 22, 1996.

17. Elizabeth Geake, "The Electronic Arm of the Law," New Scientist, May 8, 1993, p. 21.
18. National Institute of Justice, Law Enforcement for the 21st Century, National Institute of Justice, June, 1994.
19. T. Dunkle, "Newist Danger Zone: Your Office," Working Woman, August, 1994, p.34.