

HOW WILL BIOMETRICS IMPACT THE IDENTIFICATION OF CRIMINALS IN
MID-SIZED LAW ENFORCEMENT AGENCIES BY 2006?

A project presented to
California Commission on
Peace Officer Standards and Training

by

Lieutenant Timothy D. Taylor
Bakersfield Police Department

Command College Class XXXI

Sacramento, California

November 2001

This Command College 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 view and conclusions expressed in this Command College Project are those of the author and are not necessarily those of the Commission on Peace Officer Standards and Training (POST).

Copyright 2001

California Commission on Peace Officer Standards and Training

TABLE OF CONTENTS

	Page
LIST OF TABLES	iv
Chapter I	
ISSUE IDENTIFICATION	
Introduction	1
How Others Know Us	2
Unraveling Biometrics	4
Evaluating Individual Biometric Potential	11
Chapter II	
FUTURES STUDY	
Nominal Group Technique	14
Trends	15
Events	21
Cross Impact Analysis	25
Alternative Scenarios	28
Pessimistic Scenario	28
Optimistic Scenario	29
Normative Scenario	31
Why Look Ahead	32
Chapter III	
STRATEGIC PLAN	
Introduction	33
Social, Technological, Economic, Political and Legal Issues	34
Organization Analysis	37
Organization Strengths	38
Organization Weaknesses	39

Environmental Analysis	40
External Threats	40
External Opportunities	41
Stakeholders	41
Snaildarters	43
Recommendations for Implementation	43
Budget Issues/Funding Sources	45
Why Bother to Plan	47
Chapter IV	
TRANSITION MANAGEMENT	
Introduction	48
Look Before You Leap	51
Chapter V	
CONCLUSION	
Summary	53
Impact on Leadership	55
Recommendation for the Future	56
THE APPENDICES	
Appendix A	60
List of Trends	
Appendix B	62
List of Events	
Appendix C	64
Change Strategy Chart	
Appendix D	65
Roles and Responsibility Chart	
Appendix E	67
Readiness and Capability Chart	

Commitment Planning Chart

NOTES

BIBLIOGRAPHY

LIST OF TABLES

Tables		Page
1	NGT Flow Chart	14
2	Summary Trend Table	16
3	Summary Event Table	21
4	Cross Impact Analysis	26

CHAPTER ONE

ISSUE IDENTIFICATION

Introduction

Technology has created a new criminal element that society must fend off: the cyber criminal. Instead of lurking in dark alleys as shadows and stalking their prey, they sit at their computers hacking away at people's deepest financial secrets hoping to find that small oversight that permits them to have ultimate control of one's personal financial assets. Or rather, they simply steal identities through the use of optical scanners, color printers, and access to numerical identifiers such as driver's license and social security numbers. Law enforcement has the duty to protect the public from those who would do it harm and to provide the necessary information that permits society to protect itself. Yet law enforcement must also walk a tightrope that ensures it does not infringe on society's rights to individuality and personal privacy. Biometrics, more than any other form of identification, may imperil one's sense of individuality and create a mind set that government is meddling far too much in everyone's personal lives. How far does government need to go to insure individual safety and security, and at the same time respect the rights of its citizens? Answers to these questions are complicated; to rush headlong into systematic biometric verification and identification without careful consideration of how to balance personal privacy with safety and security will undoubtedly cause unintended and unforeseen circumstances in the future. The use of biometrics is no longer a scene from a second rate science fiction film: it is real, it is here, and mid-sized law enforcement agencies need to brace themselves for the impact and implications this new science brings to the law enforcement profession.

How Others Know Us

Human identification is the association of data with a particular human being. The original need for identification was social rather than economic, but as economic transactions became more complex the need arose for parties to know with whom they were dealing. In this context, the purpose for the exchange of identification was as a gesture of goodwill, to development business relationships and to minimize the possibility of dishonesty. While the term biometrics is fairly new it has been applied in a variety of ways since at least the time of the Pharaohs when a person's height was used to identify them for grain distribution.

Most people assume that their identities are established first by name and then by skin color, hair color, and eye color; height and weight; and, the ridges, loops and whorls that make up their fingerprints. These are the conventional forms of identification that have been used to distinguish humans as individuals for most of their lives. These traits are but a few that determine who and what we are. There are a variety of methods available for identifying a person. The obvious include:

Names - what others call us;

Social Behavior/Status - how we interact with others and they with us;

Title - what organizations call us;

Knowledge - what we know;

Tokens - what we have;

Bio-Dynamics - what we do;

Natural Physiology - what we are;

Imposed Physical Characteristics - what we've done to change our appearance.¹

And, there are those identifiers that are not so obvious. These non-conventional methods of identifying individuals are known as biometrics. The term means life measurement² and refers to the methodology of recognizing and identifying people based on their individual and distinct physiological or behavioral characteristics.³ Types of biometrics include facial recognition, fingerprint scanning, iris/retina scanning, voice print analysis, hand geometry and palm scanning, signature recognition, vascular pattern comparison and thermal imaging.

In 1998, the Center for Applied Research and Policy Analysis at the Metropolitan State University in St. Paul, Minnesota studied the accuracy and application, associated costs, and legal and privacy issues involved in biometrics and concluded that biometrics have enormous potential for public and private organizations.⁴

Verification Verses Identification

A biometric system is nothing more than pattern recognition that makes identification possible by determining the authenticity of a specific physiological or behavioral characteristic. Basically, identification occurs in three forms: something you have such, as a card; something you know, such as a password or number; or, your specific traits, such as the forms of your fingerprints, the tone of your voice, or the manner in which you sign your name. A biometric system can either be verification or identification. Verification confirms or denies a person's claimed identity (Am I really who I claim to be?), while identification has to establish one's identity from a group (Who am I?). Verification, or authentication, normally occurs in conjunction with tokens such as: drivers' licenses, personal identification numbers and passwords that link the token to

the holder; whereas identification occurs through the analysis of certain traits specific to the person such as fingerprints, retina scans, DNA or a combination of traits.⁵

Unraveling Biometrics

Biometrics fall into two categories: physiological and behavioral. A physiological biometric includes the face, retina and iris, fingertips, thumb, finger length or pattern, hand geometry, wrist vein patterns and thermal images. Behavioral biometrics may include voiceprints, handwritten signatures and keystroke dynamics.⁶ The effectiveness of the various biometric methods vary, some are much more convenient and socially acceptable while others are intrusive and inconvenient. Ideally, the best biometric method must be fast, non-intrusive, convenient, cost effective and as previously mentioned, socially acceptable.⁷

In recent years biometric identification has reached a very high degree of sophistication and its accuracy is now considered to be at a level that far surpasses all other forms of identification. According to Richard Norton, Executive Director of the International Biometric Industry Association, "Using biometrics actually complicates stealing by an enormous factor."⁸

The Eyes Have It

A person's eyes contain two forms of biometrics, the retina and the iris. Each are measured in different ways. The retina scan looks at the vein patterns on the tissues at the back of the eyeball, while the iris scan analyzes the tissues of the ring that expands and contracts at the front of the eye to form the pupil. The retinal scan is complex and

requires light to be introduced in the eye at close range to illuminate the veins on the retina. It is somewhat likened to having your eye doctor peer into your eyes with light during a routine exam. This form of biometric is considered highly accurate and makes it an excellent choice for high-security facilities, but it also requires the full cooperation of the person being scanned.⁹ It poses some problems for people who wear glasses or have problems with focusing in the reading device. Retina scanning technology has been improved in recent years but it still has an acceptance problem.¹⁰

Iris scanning is a much friendlier mode of biometrics that uses standard photography to capture the pattern that forms the color of a person's eye. Surprisingly, the iris remains unchanged from the time a person is 18 months old.¹¹ The scan provides a digitized template that is placed in a data processor much like a grocery store bar code. When that person requires access to a building, computer, or automated teller machine, the process repeats itself and is compared with the information stored in the database. Unlike retinal scanning, iris scanning is less intrusive, can be accomplished with eyeglasses in place and works well in applications requiring identification rather than verification.¹² In the 1993 science-fiction film "Demolition Man" the villain faced a dilemma: a lock on a science lab that was protected by a biometric device that required an eye scan to open it. The villain found a scientist, plucked out his eye and held it up to the scanner and was granted admittance.¹³ This scenario, while purely fictional, illustrates the belief many people have about the potential outcome of biometrics and their science fiction-like uses.

In a Sandia National Laboratories Report, "A Performance Evaluation of Biometric Identification Devices," it was found that biometric techniques such as retina scanning

had the most negative reaction when compared to all other methods. The invasive nature of retina scanning, which requires the user to remain still while an infrared beam is shined through the pupil of the eye significantly reduces the overall acceptance of the procedure.¹⁴

Fingerprints

Fingerprint identification is one of the oldest biometric applications. Some believe that the Apostle Paul used his fingerprints to sign his writings, and Chinese documents from the T'ang Dynasty refer to fingerprints being impressed on business documents.¹⁵ Numerous historical references have been made regarding the uniqueness of fingerprints since the 14th century. The official introduction of fingerprinting, as a means of criminal identification was devised by Sir Edward Richard Henry the Inspector General of Police in Bengal, India. The modern Henry System of ten-finger identification was born and has been used ever since.¹⁶

The Henry system divides fingerprints into three patterns: loops, whorls and arches. All ten fingers are considered a unit for the purposes of classification. The fingerprint set is then assigned a classification represented by a combination of numbers and letters for future reference.

In late 1960 the Federal Bureau of Investigation (FBI) began its efforts to automate the fingerprint processing system. The ambitious and much anticipated National Crime Information Center (NCIC) 2000 database promised field access to FBI fingerprint files so officers can confirm the identities of the people they are dealing with.¹⁷ But this new technology doesn't come without some serious costs. NCIC 2000 was

more than 90 million dollars over budget and will eventually cost state and local agencies millions of dollars to upgrade their current fingerprint systems.¹⁸ This substantial investment in technology on their behalf will place new computer terminals in patrol cars and networking equipment within their departments. As a result hundreds of hours will be spent in programming.¹⁹

While NCIC 2000 holds promise for in-field fingerprint checks, its sister system the Integrated Automated Fingerprint Identification System (IAFIS) will add a greater search dimension during the booking process. IAFIS has the capability of searching its database and providing a response to an inquiry in less than two hours; historically this process could have taken months to complete. IAFIS permits law enforcement to check individuals, arrested for petty crimes, for major crimes they may have committed in another jurisdiction or state.

The benefits of fingerprint scanners, such as live scan, is that they are harder to fool than some biometrics such as face recognition. Their ability to measure the uniqueness of a person's fingerprints makes them a convenient and trustworthy tool. The downside is the cost, which ranges between \$30,000 - \$60,000 and can strap smaller departments.

Hand Geometry

Hand geometry is a biometric based on the premise that the size and shape of a person's hand doesn't change after a certain age.²⁰ Everyone's hand has a distinct size and shape, and its three-dimensional characteristics including length, width, thickness and contour of the fingers make it possible to measure and encode.²¹ Methods of

measurement usually fall into one of two categories – mechanical or image detection.

Hand geometry was the first biometric to be used in a commercial setting.²² The device, Identimat, came on the market in 1976.²³ In 1993, United States Immigration authorities opened the Immigration and Naturalization Service Passenger Accelerated Service System (INPASS) at John F. Kennedy and Newark airports. Applicants for the program are enrolled after they are interviewed and their identities confirmed by authorities. Their palm is scanned and they are issued an identification card that permits them to by-pass the normal airport checkpoints and proceed to a kiosk where their hand is scanned and matched to the information on their identification card.²⁴

The comparison data for hand geometry is small which means that the chances of someone having the same characteristics are much greater than other biometrics such as fingerprints or eye scans. For this very reason a secondary form of identification or verification is usually required – such as the card in the case of the INPASS application.

Face Recognition

Facial recognition is the most natural means of identification – and it too is a biometric. Facial recognition is the ability to identify another individual by the various characteristics of their face, which include: ears, eyes, nose, mouth and head shape. Police sketch artists have been marginally successful at recreating facial images from witness and victim statements, and police technicians trained in using celluloid templates such as Identikit were sometimes able to get a fairly accurate depiction of suspects. It is easy for humans to identify one another, but it becomes quite a different story when computers attempt the task.

But, with new computer technology and digital imaging facial recognition is becoming one of the fastest growing biometric technologies. Hardware is not very expensive and a good facial recognition system can be run on standard personal computer hardware.

Early facial recognition systems relied on two dimensional mug files; however; new systems use object-oriented programming that incorporates three dimensional composite technology that can easily identify angle-viewed face images of subjects caught on video surveillance or still-photo cameras. In seconds, the computer matches facial features of the subject photo or video with its stored files and makes the identification. More than 60 million images can be stored on a typical desktop computer from which sixty-four facial features and fifty-six points of comparison can be made.

One important advantage of facial recognition technology is its cost; it is one of the least expensive biometric technologies. The combined price for hardware and software can be as low as \$400 per set-up.²⁵

Voice Print

Voice analysis or voice printing has not received acclaim as a biometric. The process can be slow and the quality of the sample can be affected by emotions, physical impairment due to drugs or alcohol, and illness. Voiceprints offer an excellent means of accessing databases from remote locations,²⁶ making it possible for the user to use a telephone and be some distance from the information they desire.

Voiceprint verification uses bass and treble tones, larynx vibrations, and nasal tones to establish and verify user identity.²⁷ Voice printing requires the enrollment of the

user who must repeat a set of phrases several times as the system monitors what the speaker says. From these repeated phrases a template is made that eventually recognizes the user.²⁸

Voice printing differs from speech recognition in that the computer analyzes voice patterns as opposed to trying to understand what is actually said.²⁹

Lesser Known Biometrics

One of the lesser-known biometrics includes signature recognition, which is based on the dynamics of signing your name. It analyzes how you accelerate your pen, the direction you write, pressure on the paper and length of your pen strokes.³⁰ LCI Technology Group has invented a “smartpen” device that contains a microcomputer and functions as a ballpoint pen. The “smartpen” effectively measures a person’s signature and according to Sam Asseer, chairman and CEO of LCI, “This product is the missing link in the security loop.”³¹

Another lesser known biometric is thermal imaging, which takes measurements of body heat with an infrared camera. It is extremely difficult to fool, but it also requires extremely expensive infrared cameras that make it prohibitive to own. For this reason thermal-imaging technologies are usually reserved for situations requiring ultra-high security such as nuclear facilities or specialized research laboratories.

Evaluating Individual Biometric Potential

The basic premise behind any biometric is that it provides the right amount of

security or verification, or properly identifies those individuals it's supposed to identify. How do we know if a particular biometric is capable of doing its job? False accept rates (FAR) and false reject rates (FRR) are used to gauge the identifying power of a particular biometric. FAR and FRR require exceptionally large statistical samples, most of which are hard for the industry to provide.³² The following is an example from a Recognition Systems White Paper titled, Convenience VS Security: How Well Do Biometrics Work?

A business with 100 employees has a biometric device at its front door. Each employee uses the door four times a day, yielding 400 transactions per day.

A False Reject Rate of 1.0% predicts that every day; four good guys (1% of 400) will be denied access. Over a five-day week, that means 20 problems. Reducing the False Reject Rate to 0.1% results in just two problems per week.

A low False Reject Rate is very important for most applications, since users will become extremely frustrated if they're denied access by a device that has previously recognized them.³³

False accept rates determine the probability the wrong person will be allowed access or be identified whereas false reject rates determine the probability a biometric device won't recognize or identify the proper person; the point at which these statistical curves cross is referred to as the equal error rate. Equal error rates provide an indication of an individual biometrics performance. The lower the equal error rates the better.

It is important to understand the meaning and implications of the FAR and FRR. A system that delivers optimum service, for a specific purpose, under the right condition, will deliver the intended result. If it doesn't, users will lose confidence in the system and seek out ways of evading or sabotaging it.

As with any sensitive information, safeguards such as encryption, authorization and restriction will maintain the integrity of the tool. Many new technologies are slow to catch on with the public. But, once they understand how a technology works and what its intended use is supposed to achieve, they are quick to embrace it. Biometrics still has several hurdles to overcome, which may infringe on its public acceptance and eventual use by law enforcement. First, is the acceptance factor, which goes hand in hand with educating the public and permitting them to discover how well biometrics work in their own interest. Financial institutions are beginning to experiment with biometrics as a component of their automated teller machines. Soon, iris or finger scanning may replace personal identification numbers. These types of transactions hopefully will include confidence in biometrics, allowing them to become more readily accepted. Second is regulation – or lack thereof. Currently, there are no standards by which biometrics are governed.³⁴ While abuse is rare in its present state of use, the potential for widespread abuse increases as biometrics become mainstreamed. Finally the issue of interoperability, or the ability of one biometric system to function on a variety of operating platforms.³⁵ Ideally, biometrics should have the ability to interface with each other and to perform on a number of operating systems whether on mainframe or stand-alone personal computers.

Changing crime trends, increased security needs, and acts of foreign and domestic terrorism are just a few reasons why biometrics will play a part in the future of law enforcement. Biometrics will provide law enforcement a means to enhance its identification capabilities. In doing so, potential criminal acts may be thwarted and those who are able to commit crime will be positively identified. The use of biometrics in

criminal investigations is much more sophisticated than checking for latent prints or sorting mug shots for a photographic line-up. The technology will require training and the purchase of equipment. The impact and costs to mid-sized law enforcement agencies will be significant. But, to put off the implementation of biometrics would be likened to the continued use of punched teletype tapes for warrant checks now that the NCIC 2000 computer system is on-line. Biometrics is the future of law enforcement identification and this study hopefully points the way to a means of managing or influencing that future.

CHAPTER TWO

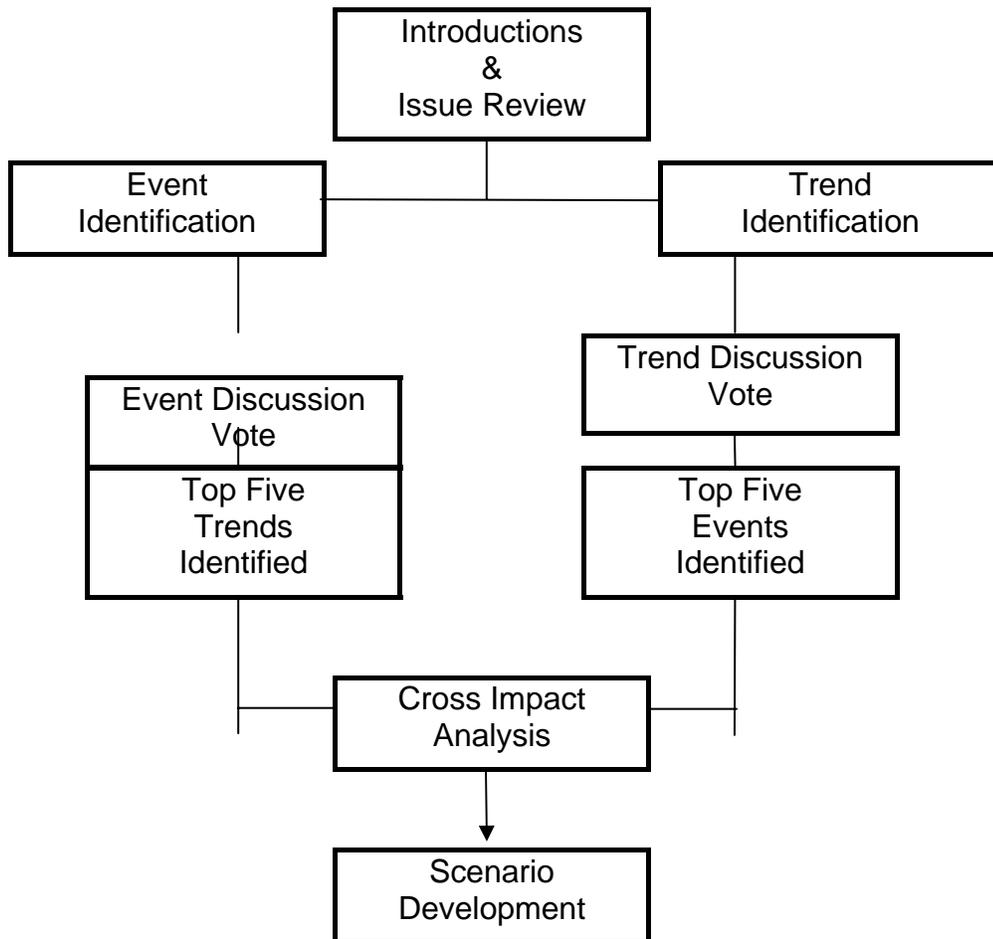
FUTURES STUDY

Nominal Group Technique

In order to examine how biometrics will impact the identification of criminals in

mid-sized law enforcement agencies by 2006, a futures study was conducted using the Nominal Group Technique (NGT) process. The following flow chart illustrates the steps in the NGT process:

TABLE 1
NGT Process



Each NGT panelist was provided background information relative to the issue. This information provided each NGT panel member with an introduction on biometrics and potential for future biometric uses. The NGT panel consisted of the following members. All were from Bakersfield:

- A police lieutenant with twenty years of varied law enforcement experience, including supervision of sexual assault investigations.
- A police sergeant with eighteen years of law enforcement experience that includes experience as a probation officer and supervision of white - collar crime investigations.
- A training officer with ten years experience, including policy development and basic police academy supervision.
- A police lab technician with twenty-five years of experience in crime science investigation and collection of evidence.
- A computer analyst and web page designer.
- The director of public safety programs at a local community college.
- The department chair from the Criminal Justice Education Department at California State University Bakersfield.
- The supervising deoxyribonucleic acid (DNA) analyst from the Kern County District Attorney's Laboratory.

Trends

The initial step in the NGT process is the identification of trends that could impact the issue. Trends are social, technological, political, economic, environmental, or legal conditions whose characteristics can be estimated or measured over time. Trends most often indicate a potential directional change in an issue and are often gradual and long term. In a round robin discussion, each panelist presented their top three biometric trends, one by one, until all trends were discussed and posted on flip charts. A total of

thirty trends were identified (Appendix A). The panel members elected and were permitted to personally choose their top five most important trends. They then focused their work on selecting, as a group, the top five trends from all identified trends. Using a score of 100 as a rating for where each of the trends is today, the panelists were asked to rate the importance of each trend as it was five years ago, will be in five years and in ten years. They also assigned a level of concern to each trend to identify how important each was to the issue. The summary trend table was then completed for the top five trends using the median scores from all of the NGT panelists' ratings.

TABLE 2

Summary Trend Table

TRENDS	-5	TODAY	+5 YEARS	+10 YEARS	CONCERNS
T-1 Privacy Issues	65	100	250	200	+8
T-2 Officer Knowledge	50	100	450	550	+8
T-3 Fingerprint Systems	50	100	300	600	+8
T-4 Big Brother Fears	77.5	100	200	225	+8.5
T-5 Crime Shift	77.5	100	200	500	+8

Trend One: Constitutional Concerns Regarding Privacy Issues

The panel identified the trend of on-going constitutional concerns over privacy issues as the number one trend in their voting. It was the feeling of the panel that

Americans have always been concerned about privacy issues and we're protective of our right to privacy and abhor government intervention in our personal lives. As biometrics are introduced into mainstream society and become more commonplace, the public's adverse reaction to their use may diminish. There will be considerable tolerance for biometrics in private industry and in issues pertaining to security. But, as the government develops uses for biometrics, the public may view this as an intrusion into their privacy and may be resistant to its acceptance. In assessing the trend, the panel concluded that trend was slightly more than half five years ago of what it is today, will be one-half times greater in five years, and interestingly enough will only be twice as great in ten years. The panel's reasoning for the decrease was that the public may grow to accept biometrics once it is proven that the government will not abuse its uses. The panel assigned a level of concern of eight to the trend indicating they thought its impact on the issue quite positive.

Trend Two: Skill and Knowledge Base of Officers

The trend of the changing skill and knowledge base of officers was determined to be highly important to the panel as well. The assignment of a level of concern of eight reflects their concern. As technology grows, and its uses become more prevalent in law enforcement, it will be important to ensure that new officers, as well as existing officers,

receive the necessary training to do their job. If biometric identification becomes widely used, officers will need to understand its capabilities, how to use the various biometric methods and be prepared to testify in court as to how it was applied to identify the suspect. Traditional training methods will shift from academically based learning to technologically based learning, and will take on a scientific twist that hasn't yet been introduced in customary police training; the panel believed that we are just beginning to see the emergence of this technological training in law enforcement circles. They felt the trend was half as important five years ago as it is today, will be four and one-half times more important in five years, and five and one-half times more important in ten years. This trend was selected by the panel to have the most positive impact on the issue during the next five years.

Trend Three: Use of Advanced Fingerprint Systems to Identify Individuals

The panel determined that the use of advanced fingerprint systems to identify individuals was of significant importance. The human fingerprint has long been accepted as a means to identify persons for a variety of criminal and non-criminal reasons. Since fingerprints are a biometric form of identification, the panel believed that the public's current acceptance of them for identification purposes would continue. What they also believed is that advanced fingerprint identification systems such as Live Scan, the Integrated Automated Fingerprint Identification System and NCIC 2000 Fingerprint Computer will continue to be developed for law enforcement use. These systems will improve over time and their use will become more prolific. Fingerprint systems as we know them today will most likely change and become less expensive, so mid-sized

agencies will be able to purchase them. Fingerprints will continue to be used for security and privileged access to sensitive information, and may even be incorporated as part of our computer passwords and login identifications. The panel members thought that the trend of using fingerprint systems to successfully identify individuals five years ago was half of that of today, will triple in five years, and grow by six-fold in ten years.

Trend Four: The Public's Fear of "Big Brother"

The public's fear of Big Brother was identified as an important trend likely to impact the issue. George Orwell's 1984 has long since come and gone, but its impact on the human psyche lingers on. This trend is somewhat related to Trend One, in that they both contain issues of privacy and governmental intervention, or surveillance. In the case of Trend One, the panelists felt that the public's fears of government supervision and management in our daily lives would create an effort to thwart the implementation of biometrics, especially the encoding of identification with specific personal data such as DNA classifications or the forced giving of genetic material for inclusion in government databases. There was a discussion about the use of red light cameras and the adverse public comments surrounding the pending implementation of those devices, which is indicative of the public's fear that government is watching and meddling in people's private lives. The panel scored the importance of this trend as fairly high five years ago, giving it a median value of seventy-seven and one-half. They thought its importance would double in five years, and increase an additional twenty-percent beyond that in ten years. Additionally, they assigned a level of concern of eight and one-half to the trend's impact on the issue, most likely due to biometrics' broad

impact on the public's anti-Big Brother mentality.

Trend Five: Sophistication of Crimes Being Committed

The fifth trend identified by the panel members pertained to the shift in the types of crimes being committed. The panel felt that a substantial shift would occur perhaps not in the short term, but most definitely in the long term. As people expand their use of the Internet for shopping and society becomes less oriented towards cash, there will be a surge in crimes that involve identity takeovers, theft of access numbers and computer fraud. The panelists felt that many property crimes such as burglary and general theft will give way to theft of access numbers such as bank ATM PINs and credit cards. Even more serious crimes such as robbery may dwindle; the rationale being – why take a chance committing a robbery and getting caught or killed for a few hundred dollars, when you can commit a computer fraud or theft and steal thousands fairly anonymously? The panel believed that this shift in crimes was fairly consistent during the last five years. The median value of their voting was seventy-seven and one-half, indicating that the trend was about one-quarter five years ago of what it is today. They thought it would double in five years, and quadruple in ten years. They also assigned a level of concern of eight to the trend, which indicates they felt it was very important to the issue.

Events

The second step in the NGT process is the identification of events that could

impact the issue. An event is defined as an unambiguous one-time occurrence. When an event occurs, our future is different. The NGT panelists were asked to identify potential future events that could impact the issue. The panelists participated in a roundtable discussion until all individual events were identified. A total of sixteen events were identified (Appendix B). Individually, the panel members voted for their top five events and then selected the top five highest rated events from the overall voting. The panel then determined the first year in which each event could occur beyond the day of the NGT and the likelihood, as a percentage, that it would occur in five years and in ten years. They then rated the impact the event would have on the issue from -10 to +10. The median scores from their ratings were used to compile the summary event table.

TABLE 3

Summary Event Table

EVENTS	1 ST YEAR>0	+5 YEARS	+10 YEARS	IMPACT -10 TO +10
E-1 Magnetic Info. Strips	7	0	50	+10
E-2 Fingerprint Databases	10	0	55	+10
E-3 I.D. Takeover	5	100	100	+10
E-4 National Tech. Policing	8	0	33	+7
E-5 Digital Tags	4	23	38	+6

Event One: Drivers License, Naturalization Identification and Passports Contain

Biometric Information on Magnetic Strip

The NGT participants felt that this was the top event among those identified in the round robin discussion. The panel felt that there was the likelihood that this event could occur, especially due to the growing concern over protecting our borders against terrorists. One panel member commented that our government could even tag citizens with digital biometric identification before allowing them to receive entitlements. Even today, our drivers' licenses contain a magnetic strip that can be scanned to verify its authenticity. The addition of biometric information is not far-fetched and could be easily accomplished. The barriers to overcome would be public acceptance and approval. The advantage to law enforcement would be a foolproof means of identifying individuals; even if they had no identification on their person, an in-field retina scan or DNA saliva test against a national database could confirm their true identity. The group felt that the earliest this event might occur would be in seven years, and that there was a fifty-fifty chance of it occurring in ten years. The impact of this event on the issue was a positive ten, indicating it would be very beneficial to the issue.

Event Two: Worldwide Fingerprint Databases Go Global and Can Be Accessed Immediately

The panel felt that since fingerprints are the most widely accepted form of biometric measurement, there would be a distinct advantage to law enforcement if worldwide databases could be accessed immediately. As portable fingerprint scanners become more available, and their technology improves, it would be nothing to identify any foreign national from the field. Obviously, one important aspect of this event is the necessity that all the world's inhabitants be fingerprinted and entered into their particular

national databases - or at least the criminals. The ability to conduct worldwide investigations into terrorism and global crimes, such as drug smuggling, would improve substantially. The panel felt though, that world political climates would undermine the fruition of this event. The earliest the panel thought this event could occur was in ten years, giving it a fifty-five percent chance that it could occur at that time. The impact on the issue was rated at ten, again indicating the panel thought it extremely important and positive.

Event Three: High Profile Criminal Assumes Another Identity

The panel determined that there was a very real potential for a high profile criminal or criminals to hack into a major identification database and assume the identity of a prominent individual. This type of crime, if discovered, would create an enormous amount of public interest in identity theft as well as an outcry for greater protection of identity and credit databases. Security measures requiring biometric measurements might add a level of safety and add to the public interest in biometric security. The panel was fairly confident that this event could occur and thought there was a one hundred percent probability it would in five years. Again, its impact on the issue would be very significant and positive as evidenced by their assignment of ten to its impact. It would demonstrate a need to implement biometrics as a personal security device.

Event Four: A National Technology Crimes Police Force is Created

The panel voiced this event as one that would be beneficial to law enforcement.

However, due to bureaucratic problems not likely to occur very soon. There is a definite need to create an enforcement/investigations unit to address the rising occurrences of technology crimes. Most law enforcement agencies at the local level do not have employees with the training or sufficient understanding of technology crimes to investigate them. Consequently, there are victims of these incidents who will never have their case investigated, much less solved. There is a lot of on-going confusion when determining who has jurisdiction over many of these technology crimes. Does the agency where the suspect lives or the agency where the victim lives have jurisdiction? This confusion frustrates victims due to the perceived lack of cooperation on the behalf of law enforcement and the victim's need for closure. The panel was not overly optimistic about this even occurring anytime soon; they estimated that it could occur in eight years. They further estimated that there was only a one-in-three chance of the event occurring in ten years. They were not as concerned about it having as positive an impact on the issue assigning it a median score of seven. This is most likely due to their skepticism that the event could or would actually occur.

Event Five: Parents Are Given the Opportunity to Digitally Tag Their Newborn Offspring

This event piqued the interest of the panel, and it seemed to create a large amount of emotion. Some equated this to the tagging of their pets with implants, while others thought the event had merit for the protection of our children. Civil libertarians would most definitely voice their concern about tagging children who had no choice or say in the matter. The inclusion of biometric information on digital tags implanted at birth could virtually eliminate child custody disputes resulting in child stealing, and many

kidnapping incidents. The panel believed that the benefits derived from the tags would not be evident for almost a generation or at least until the implanted youths started committing crimes in their adolescent years. Since the technology is available now, but not oriented toward human use, the panel determined that the event might occur in four years. There is a twenty-three percent chance that it could occur in five years, and that probability would rise to thirty-eight percent in ten years. The panelists didn't feel the event would have as strong of an impact on the issue as the other events; their assignment of a median score of six was proof of this.

Cross Impact Analysis

Once trends and events were identified, the NGT panel was asked to rate how the events, if they were to occur, would impact the trends. The panel was asked to rate the impact of the events on the trends on a scale of -5 to +5, with -5 having the most negative impact and +5 having the most positive impact. Using the median scores from their voting the cross impact table was developed. The cross impact analysis allows us to determine which event potentially carries the most impact and which event does not. It is also a basis from which futures scenarios can be developed and can be used determine which event, if intentionally caused, would have the most beneficial impact on the issue.

TABLE 4

Cross Impact Analysis

TRENDS		T-1 Privacy Issues	T-2 Officer Knowledge	T-3 Fingerprint Systems	T-4 Big Brother Fears	T-5 Crime Shift
EVENTS	E-1 Magnetic Info. Strips	-4	+2	+4	-5	+2.5
	E-2 Fingerprint Databases	+2.5	+1.5	+5	-5	+1
	E-3 I.D. Takeover	+5	+2	0	+1	+2
	E-4 National Tech. Policing	+1	+3	+2.25	+1.5	+3
	E-5 Digital Tags	-5	+2	0	-5	+1.5

In examining how each of the five events would impact the five trends, it was discovered that Event One (Magnetic Information Strips) would negatively impact Trend One (Privacy Issues) in that it would bolster the position of Constitutional Law and privacy advocates; the government already knows too much about us. Trend Three (Fingerprint Systems) was positively impacted by Event One. The panel's thinking was that fingerprint information included on the magnetic strips of drivers' licenses and other pieces of identification could eventually be accessed from the field to help officers investigate various crimes. Trend Four (Big Brother Fears) was also negatively impacted by Event One. The panel felt strongly about the relationship of Event One to

Trend Four, since there would be no escaping the hand of government once all our identifying traits become a part of our identification.

Event Two (Worldwide Fingerprint Databases) had a positive impact on Trend Three, most likely due to the relatedness of the two. If fingerprint databases were to go global, there would probably be a strong need to have an advanced fingerprint system in place to analyze, retrieve and respond to worldwide inquiries. Trend Four was negatively impacted by Event Two. It's probably safe to say it had much to do with the global effect of Big Brother fears.

Event Three (Major Identification Takeover) positively impacted Trend One in that it may cause those who are stringently opposed to any invasion of their privacy to re-think their position. This would have a very positive impact on the issue. The panel believed it may cause many of these privacy advocates to relax and acquiesce to the need of government to be proactive in seeking out alternate methods of maintaining security and ensuring that the wrong people not gain access to protected areas or information.

Event Four (National Technology Policing) had the least overall impact on any of the trends. Trends Two and Five were moderately impacted by this event. The creation of a National Technology Crimes Police Force may have some impact on the changing skill and knowledge base of officers in that they would not have to be so concerned with technology based training. The shift in the types of crimes being committed, especially high-tech crimes and computer fraud crimes would be handled by this newly created agency.

Event Five (Digital Tags) had a very negative impact on Trends One and Four. This is understandable since both trends deal with privacy issues and the government's ability to know too much about you. It was the panel's feeling that a digital implant in an infant would invoke a negative personal reaction from most people. The predominant argument being, that these babies were not given the choice of whether or not to receive an implant, a choice they never made but will have to live with for the rest of their lives. While the event negatively impacted these trends it would likely positively impact the issue. Since biometrics in a non-invasive means of identification that offers a high degree of reliability people would be more likely to accept it as an alternative to implants.

Alternative Scenarios

Scenarios are a future stories used to play out the trends and events identified by the NGT panel and are based on the information surrounding the issue as identified in Chapter One. They are provided as a "what if" model and are designed to highlight the changes that could occur based on the identified trends and events.

Pessimistic Scenario

Captain Dolby hung up the phone, "Starsky and Hutch, GET IN HERE!" The two aging detectives slowly rose from their desks and ambled into Dolby's office. "Listen, I just got off the phone with the chairman of the Charles Schwabb Corporation and they've had a major security breach," he said. Dolby plopped into his chair and continued "It seems that a computer hacker has siphoned off six billion dollars from Bill Gates' personal account and left no trace except an e-mail note that said 'Kilroy was here.' We need to catch whoever did this." Starsky looked at Hutch and asked, "What's a

computer hacker?” Hutch shrugged and asked Dolby, “So what are we supposed to do?” “Find out who did this,” said Dolby. “How?” Hutch asked. “Look, it’s 2006, you guys have been cops a long time; use your expertise and training. You’re the best detectives we’ve got,” Dolby said. “We have no idea how to do that investigation, it’s way over our heads! Call in the FBI or something” replied Starsky. Hutch asked if some of the newer officers could conduct the investigation. Dolby just shook his head no. “We have been trying to hire officers with technological skills, but there are none available, and the ones we have are so dependent on computers that they have no intuitive law enforcement skills,” he said. Hutch said, “I remember those two nerdy patrolmen who were murdered by those three prison inmates while trying to confirm their identities using a retina scanner.” “I remember that,” said Starsky. “One of the inmates had a glass eye and those two were so busy trying to get a read from it, the other two convicts got the jump on them and shot them with their own biometric handguns.” Hutch added, “Yea, the autopsy revealed the convicts used the officers’ own hands to override the safety system on their guns.” Dolby interrupted the two aging lawmen, “If you two don’t get with it, I’m gonna call in Cagney and Lacey and turn this case over to them; now get out of here!”

Optimistic Scenario

Bob Wells was watching the January 23, 2006 edition of NBC’s Dateline while preparing for his midnight shift at the Paduca Police Department. He wasn’t a big fan of the show’s liberal viewpoints and was even less excited that Geraldo Rivera had replaced Stone Phillips, who took over for Tom Brokaw, as the anchor of the NBC Nightly News.

As Wells slipped into his bulletproof neoprene jump suit, his attention was diverted by the story on television. The broadcast correspondent Mona Newmonia was deep into a dissertation about how the American Civil Liberties Union had lost a Supreme Court battle to stop prisons around the country from surgically implanting convicted felons with the Internal Registration Notification Unit (IRNU) Biometric Identifier. The IRNU implant contains DNA, fingerprint, blood type, vascular patterns, retina information and criminal history of its recipient. It allows officers in the field to quickly identify suspects with criminal backgrounds. The officer merely scans the suspect with a wand similar to a metal detection wand and it immediately registers if the person is implanted and displays his identifying information. Wells stated "It's about time the boys in wetsuits got a helping hand." He then slid his IRNU wand into its holster on his belt, slipped on his Personalized Police Firearm (PPF) Identification Ring and flipped the switch of his PPF to the "on" position. Wells kissed his wife goodnight, scanned his iris on the teleportation control panel, and was beamed into the briefing room at Paducca Police Department. "Hey Bob, how's it going?" said Ernie Thwackner, Wells' shift mate. "Good, did you catch the Dateline segment tonight?" said Wells. "I did, it was long past due," said Thwackner as he scanned his palm and opened the equipment locker. He grabbed a pair of duty boots and tossed them to Wells. "Here, you'll need these, your boots didn't teleport with you." Wells looked at his bare feet, "I hate when that happens," he said as he tried to sit down in his jumpsuit to put them on.

Normative Scenario

Detective Parker Peknobscott sat in the corner of the Sex Crimes Unit frantically searching the Megan's Law Computer for information regarding a child molester he had arrested five years ago. "Damn, this computer is slow! I wish I could access this information with my six gigahertz Palm Pilot from the field. These two gigahertz antiques from 2001 don't cut it anymore." His partner, Detective Thoroughgood Musgrave, just stared at Peknobscott. "What are you looking at?" said Peknobscott, "This computer is making me nuts!" "Exactly," said Musgrave, "Why do you let technology control you so much?" "I can't help myself – I'd be lost without my computers," said Peknobscott. Musgrave stood up and stretched, "Who is it you're looking for?" he said. Peknobscott said, "I arrested this molester, Jerry Kooy, in 2000 and I heard he was released a few weeks ago and may be back in town. The victim called me and said Jerry had called her and wanted to meet with her so he could apologize." "Ah, another remorseful reformed child 'buser," said Musgrave. "This guy is really creepy," said Peknobscott. "I think he'll harm the victim if he catches up with her, so we need to find him NOW!" Musgrave asked what he could do. "Well, I've already put it out on the Operations Division Palm Pilot frequency and I'm hoping someone stops this jerk and scans his license or identification. Putting DNA and criminal history information on drivers licenses and identification cards has done wonders for law enforcement." Just then the alert on Peknobscott's Palm Pilot went off. "Bingo, lets go," he said. "Where are we going?" asked Musgrave. "A patrol unit has our boy stopped about three blocks from our victim's home, and he has duct tape, a lock pick, and a hand sickle," said Peknobscott. "Wow, the biometrics on his identification card nailed him then," said Musgrave. "No, not exactly," said Peknobscott, "he didn't have any identification." Musgrave asked how they

knew it was Kooy without identification biometrics. “Fingerprints, good old-fashioned fingerprints,” said Peknobscott. “I told you that you relied too much on technology,” said Musgrave. “That stuff is going to get you hurt!”

Why Look Ahead?

No one can predict the future, but by actively participating in futures studies leaders may be able to foresee the trends and events that impact them. Writing optimistic, pessimistic or normative scenarios, while awkward at first, allows for deep analysis and offers a creative method for dealing with situations before they come to fruition. They help leaders formulate alternatives to problems before the problems exist. Looking ahead and planning for consequences is a giant leap toward managing the future and more importantly, appropriately responding to and managing crises. When used effectively, futures studies can be an integral component of meaningful strategic planning. It permits an organization and its leaders to prepare and respond for the most unlikely of circumstances. And better yet, it enables them to steer the organization in a direction they, and not someone else, want it to go. The next chapter focuses on the development of a strategic plan that will help mid-sized law enforcement agencies move toward managing a future that includes biometric identification in criminal investigations and as an aid in the security of the citizens they serve.

CHAPTER THREE

STRATEGIC PLANNING

Introduction

The purpose of strategic planning is to provide a structured approach, either rational or non-rational, for bringing anticipations of the future to bear on today's decisions. Many times this process is used to determine if the organization is moving in the desired direction and if its programs are receiving the necessary resources. And, to establish budgets and set operational goals, enhance coordination among its divisions, sections and units, establish accountability, and finally to take control of the organization.

Social, Technological, Economic, Political and Legal Issues

In order to anticipate the impact of biometrics on mid-size law enforcement agencies by 2006 it is important to first examine those areas that may have the greatest effect. This can be accomplished by scanning the social, technological, economic, political and legal ramifications, otherwise known as STEPL, of biometrics on law enforcement and society. Once these issues are identified it allows the organization to determine when best to transform itself and to possibly foresee potential impacts caused by the transformation. This process also permits the law enforcement agency to respond appropriately to the positives and negatives of the change, or to remaining status quo.

Social

Biometrics has no established governmental protocols or use. As well, no

industry standards have been implemented for the development of biometric measuring devices. These issues alone will impact the widespread use of biometrics in law enforcement. Society wants to be insured that government is not going to be overly intrusive; therefore, the lack of regulation will make the public skeptical about using biometrics. As the learning of individual users increases and regulations are established governing the technology, public mistrust should diminish.

The introduction of biometrics into our daily lives, as with teller machines, will increase the comfort levels of the users. Once people know how a biometric systems work they will come to realize effectiveness and value of the technology.³⁶ However, biometrics more than any other identification or verification system imperials our sense of individuality³⁷ because it uses a part of us instead of something about us. For this very reason, users will want to be insured that those parts remain private and protected.

Technological

Biometrics technologies that are used for specific purposes may achieve a certain level of confidence from the use.³⁸ Law enforcement officers, by nature, are skeptical individuals and they will want to know that biometrics can be trusted to deliver the intended results. The potential benefits of any biometric, especially when integrated with a second biometric is improvement in administrative costs, identification and verification, access to information, and overall security.³⁹

All forms of identification are opposed in some form or another at some point in time. The greatest degree of public distrust is associated with biometrics due to its invasive nature.⁴⁰ As with any technology, mismanagement will result in undesired and

unanticipated consequences.

Economics

Since most biometrics, excluding fingerprints, are relatively new to law enforcement the economic impact of their acquisition is untested. Some systems such as facial recognition can cost as little as four hundred dollars while a thermal imaging system can cost hundreds of thousands of dollars.⁴¹ As with any commodity, competition in the market and consumer demand dictates price structure of the item. As biometrics become more commonplace, their prevalence is likely to drive down the price allowing more systems to be acquired by mid-sized law enforcement agencies. Even if law enforcement doesn't create its own market niche, private businesses such as financial institutions and the gaming industry will create an enormous market⁴² and possibly drive down the acquisition price of many, if not all, biometric devices.

Many mid-sized law enforcement agencies are facing a forced conversion to biometrics via the NCIC 2000 computer. The cost to these agencies is estimated to be \$30,000 - \$60,000, plus programming and data entry costs.⁴³ Many departments, large and small, have not planned for the purchase of the hardware and software that will provide the interface between their departments and the FBI's national computer.

Political

The increase in Internet-based theft will create an even stronger interest with politicians at every level of government. They will have to walk that tightrope that

separates an individual's right to privacy and the government's need to protect its citizens. The burgeoning number of complaints due to cyber crimes and identity takeovers will force the government to promulgate laws that deter Web-based crime through the use of biometrics. These laws will give law enforcement added tools to fight these crimes, but the government will be cautious in its overall approach so as to safeguard individual privacy. As government approves the widespread use of biometrics, political action committees and public interest groups will be vocal about the perceived loss of privacy and a government shift toward Big Brother.

Legal

As law enforcement is granted the right to use biometrics beyond that of fingerprinting suspects, it will need to be cognizant of those inalienable rights guaranteed by the fourth amendment to the U.S. Constitution. It has long been true that suspects have no right to refuse to give their fingerprints and recent legislation has made it possible to retrieve DNA samples from individuals convicted of certain offenses. As biometric uses expand, there will be an expectation by the public that their personal biometrics will be held in the strictest confidence and not be misappropriated for uses beyond which it was first intended. There is legal precedence established by the California Supreme Court in *Perkey v. Department of Motor Vehicles*, that indiscriminate use of fingerprint records violates privacy rights.⁴⁴

Organizations such as the American Civil Liberties Union (ACLU) argue that police cannot take a person's fingerprints without probable cause. According to Barry Steinhardt, Associate Director of the ACLU, "The Technology would almost inevitably be

used in a racially discriminatory [manner], given the ways police make decisions on whom to stop.”⁴⁵ It is highly probable this issue will occur no matter which biometric law enforcement finds most beneficial and puts into use. As with any sensitive information, safeguards such as encryption, authorization and restriction will maintain the integrity of the tool.

As mentioned, the scenarios in Chapter Two have been written to be representative of the trends and events identified by the NGT panel. The purpose of these scenarios is to function as a means of developing insight for law enforcement administrators so they can better prepare organizational visions and position their departments for change. Failure to properly prepare for change initiatives will produce consequences that could stall the progress of the agency. For the purpose of the project the normative scenario will be used as a basis to develop a strategic plan for change.

Organization Analysis

An important component of any strategic plan is an organizational analysis that examines the strengths and weaknesses of the organization using the issues discussed in the STEPL model from Chapter One. What occurs in this organizational self-examination is the emergence of strategic issues that help the organization develop its mission and values, and key strategies for implementation of a strategic plan. What

follows are the organizational strengths and weaknesses that affect the issue of how biometrics will impact mid-sized law enforcement by 2006.

Organization Strengths

1. Law enforcement is comprised of hardworking dedicated individuals who as a whole are concerned about maintaining the rights of those it serves.
2. Law enforcement is a flexible profession that is able to change direction without excessive re-tooling.
3. Mid-size law enforcement agencies often build an information network as a clearinghouse for ideas.
4. Law enforcement readily accepts training that is designed to make their job easier.
5. Law enforcement possesses a unique code of ethics that lends itself to the professional nature of the job and garners further community support.
6. Most law enforcement agencies are creative in their approach to problem solving.
7. California law enforcement is typically considered a trendsetter for developing new ideas in policing.
8. California law enforcement has established standards for hiring, certification and training through the commission on Peace Officers Standards and Training.
9. Technology grants are available through Department of Justice Community Oriented Policing Services Grants and Local Law Enforcement Block Grants.
10. Law enforcement in California has the opportunity to partner with private business, especially those in the technology industry.

Organization Weaknesses

1. Law enforcement in California is mostly reactive rather than proactive and as a result may not be as forward thinking as it could be.
2. Most California law enforcement agencies have no assigned experts to conduct thorough research on issues relating to technology.
3. Law enforcement relies on individuals outside the agency for information on funding sources such as grants and rarely has in-house personnel who are adept at grant research, writing and acquisition.
4. Law enforcement officers in general are resistant to change.
5. California law enforcement has no statewide standard for technology acquisition such as in records management systems or computer aided dispatch; consequently systems from one department to another do not interface.
6. While California law enforcement readily shares information, they rarely create inter-agency partnerships that allow for the pooling of resources and consolidation of services.
7. Law enforcement in general is frequently at odds with local, state and federal legislators over mandated regulations.
8. Law enforcement is reluctant to ask for help from non-law enforcement entities such as private business, and it rarely makes use of consultants.
9. Local law enforcement frequently competes for funding that is substantially less than needed to acquire new technology and is hamstrung by cumbersome bidding and proposal rules for purchase.

10. Law enforcement is not very vendor savvy and is frequently promised and pays for a product that vendors cannot deliver, often without recourse.
11. Many law enforcement agencies have no strategic plan in place to guide the organization and as a result they are crisis driven.
12. Law enforcement rarely recognizes the importance of stakeholders early on in a project and is normally reluctant to garner their support.

Environmental Analysis

The organizational analysis examines the strengths and weaknesses of the organization from an internal perspective and allows for the evaluation of the issue through bureaucratic criticism. On the other hand, the environmental analysis examines the external threats and opportunities the organization must consider in order to develop strategic plans for change.

External Threats

1. There is a persistent and on-going public fear that government is too involved in our personal lives.
2. There is a general lack of knowledge in both public and private sectors about biometrics and how they can serve as a useful tool.
3. There are no protocols for use or industry manufacturing standards to biometrics.
4. Occasional but unanticipated occurrences, such as a power crisis or dramatic fuel increases, which affect the organization's discretionary spending.

5. There are forced political mandates that focus on sociological issues and steer departments away from technological advancement or at the very least delay it.
6. There are mandatory changes, such as the NCIC 2000 computer conversion, that force an agency into hurried change without sufficient time and resources to manage it.

External Opportunities

1. The increase in the number of Internet crimes being committed and the lack of trained investigators or jurisdictional oversight.
2. The need of biometric companies to gather large amounts of statistical information to evaluate their product performance.
3. Public/private partnerships that can provide goods and services to those law enforcement agencies who may not have the internal resources.
4. Capitalize on the reduction in the armed forces by actively recruiting retired defense department experts as biometric consultants.
5. Make use of involved citizens through the creation of focus or advisory groups and/or citizen training academies.

Stakeholders

Stakeholders are groups or individuals who are either impacted by what we do, or impact what we do as an organization. In order to determine what impact biometrics will have on law enforcement by 2006 it is vital that the potential stakeholders will have an influence on the success of an organization's transition to biometric identification or

verification, and in the overall strategic plan for implementation. In the context of the normative scenario these stakeholders may include:

1. City Council/Board of Supervisors
2. City Manager
3. The Chief of Police
4. Department Command Staff
5. California Department of Motor Vehicles
6. Federal Bureau of Investigation
7. California Department of Justice
8. Department Middle Management
9. Department Supervisors
10. Department Uniformed Personnel
11. Department Technology Consultant
12. Management Information Department
13. Civilian Personnel
14. General Public
15. Criminal Suspects

Along with identification of the stakeholders it is important to identify each of them as either a change strategist - those who identify the need for change; or change implementors - those who manage the day-to-day process of change; or a change recipient - those who must adopt and adapt to the change.⁴⁶ The change strategy chart (Appendix C) analyzes the stakeholders in these terms.

Snaildarters

Snaildarters are unanticipated stakeholders who can impact the issue. It is always important to take these individuals into consideration when developing a strategy for change. In the case of biometrics implementation, these snaildarters may surface as right to privacy and antigovernment groups who oppose the use of technology in society or perceived infringement upon personal freedoms. These groups may include:

1. The Green Party
2. Earth Liberation Front
3. American Civil Liberties Union
4. National Urban League
5. Amnesty International
6. Ku Klux Klan
7. Human Rights Watch

It is not necessary to include groups such as these in the implementation plan, but it is wise to anticipate the impact they could potentially have on bringing a change, such as investigative use of biometrics, to fruition. In this case, each could have individual motives for wanting to thwart the organization's desires.

Recommendations for Implementation

The following represents identified recommendations for implementing biometric technology within a mid-sized law enforcement agency:

- Identify the specific need or problem to be addressed with a biometric.
- Determine if the need is relevant to the agency's strategic plan.

- Identify stakeholders and snaildarters.
- Create teams to conduct research.
- Identify specifications/standards required to achieve the desired objective.
- Investigate what other agencies are doing to deal with the problem.
- Keep employees at all levels of the organization informed and actively seek their input.
- Enlist the support of executive management such as the City Manager.
- Enlist the support of the governing body.
- Investigate funding sources, both internal and external.
- Develop a project time line for research and acquisition of the equipment.
- Find reputable vendors and have representatives demonstrate their product.
- Carefully evaluate the individual biometrics features.
- Determine if it adequately addressed the need or problem.
- Identify the implications of its use, internally and externally.
- Evaluate cost vs. benefit.
- Arrange training for all users.
- Ensure necessary technical support is provided.
- Conduct a long range cost assessment.
- Check for compatibility with an existing information system infrastructure.
- Involve legal experts in the contract process.
- Develop policy and procedure of use.
- Do site visits to other agencies and interview product users; ask specific questions about the vendor.

- Acquire funding.
- Purchase and install the system.
- Monitor, evaluate and adjust as needed.

Budgetary Issues / Funding Sources

With the exception of fingerprinting, most biometric identification has never been extensively used in law enforcement. Since the technology is new and just beginning to make its impact known to society and law enforcement, it is hard to anticipate the future economic impact biometrics will have on our profession. The lack of established standards for biometrics in law enforcement and the absence of structured laws to govern their use deters hastened implementation. Depending on their identified use, a complete biometric system can cost anywhere from a few thousand dollars and up, to the tens or hundreds of thousands of dollars.

Since biometric systems can be expensive to acquire, it is important that careful planning take place prior to their acquisition. Many agencies may want to take advantage of technology grant opportunities through the Department of Justice (DOJ), the Office of Justice Programs (OJP) that includes COPS MORE grants, supplemental law enforcement block grants and California Law Enforcement Equipment Program grants. Other possible sources include private funding via such avenues as corporate, community, family or special purpose foundations. Some biometric companies may provide their product in order to gather statistics on its performance; while this may give the organization a chance to test the worthiness of the device, it probably is not a responsible manner of acquiring it.

Agencies having a strong interest in using grants to acquire this new technology

should contact the various sources and ask to be included on their mailing lists and electronic notifications. The Internet offers a wealth of information on potential funding opportunities. Most government agencies offering grants to law enforcement can be accessed via their Web sites. Information on these funding agencies can be obtained using the National Criminal Justice Reference Service (NCJRS) Justice Information Web site at (ojjdp.nccjrs.org/grants/grants.html), The Grantsmanship Center's Web site at (tgci.com) and The Foundation Center's Web site at (fdncenter.org).⁴⁷

There are many resources that law enforcement can access for grant assistance; these references include, Associated Grantmakers, The Chronicle of Philanthropy and, the International Chiefs of Police publication titled, "Grant Writing: A Best Practices Guide," that provides pointers in research, writing and formatting grants.⁴⁸ Grant writing is an art and most law enforcement agencies lack the skilled personnel to successfully acquire funding through the grant writing process. These agencies should seek the services of a professional grant writer or grant consultant to enhance their opportunities for success.

Before funding is secured and biometric equipment is obtained and implemented, consideration must be give to training costs, system maintenance and replacement cost of the system. These expenditures may be paid through the agency's normal operating budget, incorporated in the grant request or reimbursed by oversight agencies such as the California Commission on Peace Officer Standards and Training (POST).

Why Bother to Plan?

The strategic plan forms a foundation for transition. It becomes the roadmap that guides the way for the organization and its leaders. In order for any strategic plan to

work it must be flexible and dynamic, rather than rigid and static. It gives the organization an opportunity to be introspective and honest about its strengths and weaknesses. The plan allows for the identification of opportunities and threats making it possible to capitalize on those opportunities and counter those threats that may make the difference in a successful organizational transition to the use of biometrics. Think of the strategic plan as a blue print to build a successful learning organization that embraces change and builds consensus among its participants.

CHAPTER FOUR

TRANSITION MANAGEMENT

Introduction

It is important for an organization to develop a plan of transition to manage change effectively. Law enforcement organizations are no different in this respect. Sticking to a critical path, that includes six distinctive sequenced steps, the law enforcement manager can achieve a degree of task alignment that develops a cycle of commitment, cooperation and competence. The law enforcement agency that desires a transition from token-based identification and verification or the introduction of biometrics as an investigative tool must ensure a smooth transition through proper task alignment. Consider these six steps:

Diagnose the problem. Current methods of identification and verification are becoming antiquated, and subject to forgery and fraud. The Internet has created a new forum for criminals to take advantage of almost anyone at anytime. The FBI NCIC 2000 computer is on-line; however, the majority of law enforcement agencies have not developed a plan to acquire the necessary equipment to use the system effectively. Terrorist acts and indiscriminate acts of violence are a reality and are likely to occur at anytime. The public has a high level of concern for their right to privacy, but also wants to be protected from those who prey on them. Once the problem has been identified, it becomes critical to involve a committee of organization stakeholders to define how the organization can better manage the change. These committees or teams must also be charged with

alternatives that adequately address this issue.

Develop a Shared Vision. The law enforcement agency that makes the decision to adopt biometrics as a part of its operational plan must define the roles and responsibilities of those involved in the change. Defined roles and responsibilities allow for the delineation of work and provide for less resistance through the open flow of information and the development of a shared vision.⁴⁹ Once the role of the stakeholders have been identified, it is important to define the project responsibilities to those individuals. Clarifying these responsibilities can serve to reduce ambiguity, wasted energy and adverse reaction to the plan;⁵⁰ it also adds an important element of inclusiveness to the strategic plan implementation. Critical mass is achieved when individuals at all levels of the organization commit to the proposed change. At this point the leader moves the employees toward a vision that defines their roles and responsibilities in the changed organization. The roles and responsibilities of the stakeholders for the issue are listed on the table (Appendix D).

Foster Consensus. The implementation of any new technology can be a daunting task. Almost everyone is resistant to change and it usually occurs in varying degrees. Frequently this resistance comes from the lack of knowledge and training. At this point, it would benefit the department to train its employees on the use and capabilities of biometrics. From this training, the employees develop skills that motivate them to support the transition. This may also be the point at

which some of the more senior personnel, especially at the management level, need to be reassigned. Replacement of individuals who outwardly resist change sends a message that the department is committed to change. The readiness chart (Appendix E) identifies the stakeholders and ranks their perceived readiness and capability with respect to the change.

Spread Revitalization Without Pushing it from the Top. When a law enforcement agency initiates change, it is important to determine the level of commitment necessary for the change to be successful. This may mean taking the time to examine the various levels of authority that exist to help the change along. Many law enforcement managers try to force the change on their subordinates without giving consideration to the commitment required from them. Giving certain stakeholders a sense of ownership creates commitment. In order to elicit the requisite commitment, it is necessary to understand the resistance that may prevail. The levels of commitment common in change are:

Let It Happen;

Help It Happen;

Make It Happen.⁵¹

The commitment chart (Appendix F) summarizes the level of perceived commitment of each of the issue's stakeholders in adopting and adapting to a biometric system.

Policies, Systems and Structures. Once the stakeholders are committed to

implementing biometric systems, understand their capabilities, and are trained in their use, it becomes necessary to introduce policies, systems and structures into the organizational environment. Policies will need to be drafted that govern the use of biometrics and the ramifications of abuse. These policies would establish formal control protocols for training, release of information, collection of information and the procedures for documenting problems or failures. Systems and structures would deal with such things as the placement of a particular biometric device within the organization and the determination of its purposes, either identification or verification. Additional considerations to take into account would be how multiple biometric devices might interface with each other or how any singular biometric might interface with other equipment within an organization's infrastructure.

Monitor and Adjust. Constant monitoring by management of the system and follow-up with its end users will ensure that biometrics will become an institutionalized tool that provides long term benefits to the organization.

Look Before You Leap

Many law enforcement agencies may turn to various biometric technologies, such as face recognition, to solve on-going crime problems in crowd-prone business districts and to identify violent protestors at public demonstrations. But unlike fingerprints, which met with little or no dissent when introduced as a law enforcement tool a century ago, biometric identification will be met with vehement disapproval by certain groups who

argue that their right to privacy far outweighs any biometrics benefit to law enforcement. Currently, technology outpaces public policy ⁵²and consequently the urge to move forward to take advantage of the technology, without fully thinking things through, is one of its pitfalls.

As the cost of biometric hardware plummets, the desire to make use of its crime fighting advantages will seem to outweigh any political or social ramification. The perceptive law enforcement leader will be cautious in implementing biometric technology and will make use of all his or her available resources to make an informed decision to implement biometrics. Public unrest and mistrust of law enforcement are the obvious outcomes of impatient implementation; full-blown foreign and domestic acts of terrorism are possible outcomes due to the lack of implementation.

The next chapter summarizes the ramifications of biometrics on mid-sized law enforcement and focuses on the leadership impacts and recommendations for the future.

CHAPTER FIVE

CONCLUSION

Summary

Biometric technology will play a part of the future of law enforcement. However, not every available biometric system may have applicable uses in identifying criminals. Iris and retina scanning are difficult to fool but they are intrusive and inconvenient. Their target group would most likely include detention and correctional facilities and law enforcement agencies requiring strict access control. Hand geometry has the benefit of small storage requirements and intuitive operation but it is slow and less accurate than some of the other available biometric systems. Its uses might include facility security and area access such as property room and crime lab admittance. Facial recognition offers the greatest possible law enforcement use. It is fast and one of the least expensive methods on the market. Nonetheless, the system can be fooled by poor lighting and some disguises worn by subjects to be identified. These high-tech mug shots used in conjunction with fingerprinting could dramatically increase law enforcement's ability to identify not only petty thieves such as shoplifters but also serious felons such as bank robbery suspects and terrorists. Voice print analysis is inexpensive and has remote applications, but can be affected by the user's physical condition or emotional state. Possibilities for its use may include field investigations where officers are required to remotely access database information. As voiceprints improve, officers could be registered in communications systems and identified by their voice as opposed to a call sign. Signature recognition is an inexpensive biometric

system also affected by the user's physical condition and emotions. As law enforcement becomes more computerized and paperless, signature recognition will be used for a variety of reasons. Officers can sign for their reports and law violators identified by their electronic signatures. Thermal imaging is the most secure of the biometric systems. It is extremely hard to fool but requires expensive infrared cameras. Its potential uses would include areas requiring ultra-high security, such as courtrooms, and property and equipment storage involving munitions, narcotics and money.

Fingerprinting will continue to flourish as a law enforcement biometric identification. Its low cost and high degree of reliability will keep it around for some time. The manner in which fingerprints are collected, analyzed and compared has changed dramatically from printing to scanning, but their reliability and public acceptance continues to make them the premier identifier. The general public may have little tolerance for being subjected to certain biometric analysis, but the application of certain biometric systems in conjunction with tried and true methods will ease the public's "Big Brother" concerns and fears that government is being overly intrusive.

Biometrics has proven to be effective in many applications outside law enforcement. Casinos, state welfare systems, airport security and airline ticketing and border control have cut costs by having biometrics perform the work of several employees. Traditional investigative techniques have worked well for law enforcement but it is time to give serious consideration to taking the next step toward making technology work to our advantage as well. We need not abandon our experts and best practices for the sake of technology. Yet, we must integrate and fuse those things that work to our advantage in order to become more efficient and effective in arresting law

violators, preventing crime, and protecting those we serve as well as their personal information.

Impact on Leadership

The leader who wishes to make any transformational change must be fully aware of how that change affects everyone in the organization and the impact change has upon them. Incorporating biometrics into a department's daily routine as a security precaution, investigative tool, or both, imposes significant cultural ramifications on the organization. This type of change may appear fairly innocuous on the surface but will likely be perceived as an invasion of privacy or worthless endeavor that will soon become passe as have so many other change initiatives.

Many of today's savvy leaders may not be as technologically astute as they should be and may tend to abdicate their leadership to someone of lesser authority within the department. This transfer of power and decision making has occurred frequently and very often results in the purchase of technologies that fall short of their intended purpose or promised performance. The organization's leader must not only be a champion of the change initiative; he or she must be an informed participant as well.

Since change has such a tremendous psychological impact, it's important that the leaders develop a top-down mindset within the organization and proactively see the commitment from other recognized leaders within the organization. The leader has to make it known and obvious to everyone within the agency that the change is necessary, beneficial and warranted. This means that the leader must ensure that the appropriate level of mentoring, coaching and training occurs to build technical competency at all

levels within the agency. Frequently, crime fighting programs and tools are introduced with the expectation that the end-user will be motivated to self-train, use, and be an advocate for the program or equipment; this method of introducing a change to an organization sets the stage for failure long before the change ever occurs.

Once biometrics are implemented, the organization and its leaders must review the outcomes to insure that the desired results are being achieved without infringing on the personal freedoms of those subjected to the technology. Achievements must be recognized and rewarded, and policies and procedures reviewed regularly to optimize system performance. As this cycle continues, the leader builds a cohesive team mentality and consensus among members of the organization that eventually, changes the culture.

Recommendations for the Future

Any mid-sized law enforcement agency can implement biometric systems in their day-to-day operations. And, without a doubt biometrics will achieve certain results – both desired and undesired. In planning for a future change to biometrics identification or verification, the following steps should be taken into consideration:

- Conduct environmental scans using **STEEP** or **STEPL** to assess the community's needs, wants and desires.
- Align the agency's mission, vision and values to afford maximum buy-in by all involved in the change.
- Identify core strategies for achieving the goal.

- Develop a set of quantifiable measures for success.
- Develop a set of alternatives that allow for flexibility in case some change strategies don't work.
- Abide by an implementation plan that sets timelines accountability for, role and responsibility.
- Properly allocate resources to insure system acquisition. This includes the investigation to outside funding sources.
- Develop recognition and reward systems that honor those committed to the change.
- Communicate the plan continuously so that everyone in the organization understands the process, need, benefit and desired outcome of the change.
- Conduct regular meetings with key change implementers for progress reports and suggested implementation improvements.
- Form partnerships with the community and other government agencies in an effort to share information and gain outside support.

The world is changing at an ever-increasing rate. There are times when it seems impossible to keep up with technology and its social implications. Biometrics will definitely improve law enforcement's ability to apprehend criminals and at the same time provide society with an added measure of protection against today's sophisticated thieves, con artists and cyber crooks. The public we serve has to be assured that these very personal forms of identification and verification will be used according to their intended purpose and never for selfish or personal reasons.

Law enforcement leaders need to be proactive in the implementation of biometric systems in order to fulfill their departments' missions. This means that they must seek as much information as possible about the various biometrics at their disposal and create a vision or desired future state that incorporates the technology into the strategic plan for their department. The implementation of any change cannot and must not occur in a vacuum; the law enforcement leader must include himself or herself, the final recipient, and everyone in-between in the decision making and transition process. Trust is a big part of change and the way trust is built is by practicing the politics of inclusiveness. This inclusiveness should pertain not only to members of the organization but also should pertain to community representatives that are trained and educated in the use of biometric systems. They are an important constituency that must be afforded the opportunity to participate in the process.

The probability of an error free biometric system that offers immediate results is highly unlikely. The possibility of a completely computerized biometric system for law enforcement in the near future is remote as well. The most likely possibility will include an interface between the technology and expert technicians who will interpret biometric system matches. Letting the automated system reach its conclusion as to the subject's identity, and then permitting an expert make the final determination will provide the appropriate checks and balances to the identification process that will ease the minds of our distrustful society.

The impact biometrics offers to law enforcement is potent, but potent in many respects. It promises personal security and criminal identification beyond anyone's wildest imagination and yet excites the potential for civil unrest more than any other

technological advancement in recent history. Its advantages for law enforcement will only be realized once the public is sure that the benefit of its protective ability far outweighs its intrusive reputation. How different would the events of September 11, 2001 have been if law enforcement agencies in this country used biometrics to identify airline ticket holders or to identify foreign nationals entering our country? The answer to this question will never be known. The importance of the lesson is to insure tragic events such as those do not repeat themselves. The impact of biometrics on law enforcement will be significant so mid-sized agencies must be prepared.

APPENDIX A

List of Trends

- Fingerprint Recognition Databases
- Hand Geometry
- Facial Scanning for Identification at Large Venues
- Increased Internet Security Using Biometrics for Access to Secure information
- Digital Implants
- Biometric Research to Identify Individuals Using Body Odor, Vein Patterns, etc.
- Criminal Migrating to Smaller Communities for Anonymity
- Growing More Receptive to Role of DNA
- Biometric Identifiers Used in conjunction with Signatures
- Smart Widely Used
- Human Cloning Creating Multiple Individuals with Same DNA
- Facial Recognition Systems/Cameras at Intersections
- Verification vs Identification – Security and Internal vs Confirmation for Personal Access
- Constitutional Concerns
- Greater Reliance on Private Industry for Biometric Expertise
- Shift in Types of Crimes Being Committed
- Decreasing Cost of Biometric Technology Equipment Allowing Smaller Agencies to Purchase Equipment
- Counter Biometrics Availability on Streets/Black Market

- Identity Theft more Prevalent
- Departments Becoming More Complex – Needing Officers to Be More Technologically Savvy
- Ongoing Fraud – Virus induced Allowing Access
- Use of Biometrics Will Limit Officer Discretion
- New Database Emerging That Includes All Aspects of Biometric Identification
- Law Enforcement Technological Security to limit Access
- Political Intervention Preventing Law Enforcement Agencies from Utilizing Biometric Information
- Convenience vs Inconvenience – Are We Creating a Monster with Too Much Technology
- Skill and Knowledge Base of Officers Drastically Changing
- Reliance on Technology vs Street Skills
- Introduction of Scientific Intervention that Questions the Validity of Current Methods

APPENDIX B

List of events

- Global Monetary Computer Crashes
- Widespread disagreements Breakout Over Biometric Identification Standards
- Drivers' License, Naturalization Identification and Passports contain Biometric Information on Magnetic Strip
- State Mandates Academies Shift from Traditional Curriculum to Technology Oriented Curriculum
- Megan's Law Database Goes On-line Via Internet
- Parents are Given the Opportunity to Digitally "Tag" Their Newborn Offspring
- Flawless, Perfect identification System Invented Which Eliminates All Fraud
- All Parolees are Implanted With Global Identification System Digital Chips
- Border Crossing Identification Goes Biometric
- DNA Scanner invented and Retrieves DNA Evidence at Crime Scenes
- Legislature Passes Bill Offering Biometric Identification Equipment and Training to Departments Free of Charge
- Government Passes Law – All U.S. Citizens must be Digitally Tagged to Receive Entitlements
- Street Surveillance Cameras Become Commonplace and Widely Used
- Worldwide Fingerprint Databases Go Global and Can Be Accessed Immediately
- A National Technology Crimes Police Force is Created
- Criminal Information Linked to Everyday Activities – Limits Freedom

- Major Identification Database is Hacked and a High Profile Criminal Assumes Prominent Person's Identity

APPENDIX C

CHANGE STRATEGY CHART

		Change Strategist	Implementor	Recipient
1.	City Council / Board of Supervisors	X		
2.	City Manager	X		
3.	The Chief of Police	X		
4.	Department Command Staff	X		
5.	California Department of Motor Vehicles		X	
6.	Federal Bureau of Investigation		X	
7.	California Department of Justice		X	
8.	Department Middle Management		X	
9.	Department Supervisors			X
10.	Department Uniformed Personnel			X
11.	Department Technology Consultant		X	
12.	Management Information Department		X	
13.	Civilian Personnel			X
14.	General Public			X
15.	Criminal Suspects			X

APPENDIX D

ROLE AND RESPONSIBILITY CHART

Decision/Actor	City Council	City Manager	Chief of Police	Command Staff	California DMV	FBI	California Department of Justice
Identify Critical Issues	S	A	A	R	S	S	S
Determine Need for Change	I	I	R	S	-	-	-
Provide Strategic Plan	-	I	A	R	S	S	S
Make the Plan Happen	S	S	A	I	-	-	-
Conduct Research	-	-	S	S	S	S	S
Hire Biometric Consultant	A	I	R	S	-	-	-
Determine Specific Biometric Need	-	-	A	R	S	S	S
Select Vendor	A	I	R	S	-	-	-
Develop Goals	-	-	A	R	-	-	-
Establish Funding	A	I	R	S	S	S	S
Develop Budget	A	I	I	R	-	-	-
Policy and Procedure Design	-	-	A	I	-	-	-
Train Users	-	-	I	S	S	S	S
Institute Change	S	A	R	I	I	I	I
Provide Feedback	-	-	S	S	S	S	S

R = Responsible for decision/action. A = Approves decision/action + veto power. S = Supports decision/action only. I = Informed of decision/action only. (-) = Irrelevant to decision/action.

APPENDIX D (Continued)
ROLE AND RESPONSIBILITY CHART

Decision/Actor	Middle Managers	Supervisors	Uniformed Personnel	Dept. Tech Consultant	MIS Department	Civilian Employees
Identify Critical Issues	S	S	S	-	-	S
Determine Need for Change	S	S	S	-	-	S
Provide Strategic Plan	S	S	S	S	S	S
Make the Plan Happen	R	S	-	S	S	-
Conduct Research	S	-	-	R	S	-
Hire Biometric Consultant	I	I	I	I	R	I
Determine Specific Biometric Need	S	S	-	-	-	-
Select Vendor	I	I	I	S	S	I
Develop Goals	S	S	-	-	-	-
Establish Funding	S	-	-	S	S	-
Develop Budget	S	-	-	-	-	-
Policy and Procedure Design	R	S	S	S	S	S
Train Users	S	-1	I	S	S	-
Institute Change	S	R	-	S	S	-
Provide Feedback	I	I	R	S	S	R

R = Responsible for decision/action. A = Approves decision/action + veto power. S = Supports decision/action only. I = Informed of decision/action only. (-) = Irrelevant to decision/action.

APPENDIX E

READINESS AND CAPABILITY CHART

	Readiness			Capability		
	High	Med.	Low	High	Med.	Low
City Council/Board of Supervisors			X		X	
City Manager			X		X	
Chief of Police		X			X	
Department Command Staff			X		X	
California DMV			X		X	
Federal Bureau of Investigation		X		X		
California Department of Justice		X		X		
Department Middle Managers			X		X	
Department Supervisors		X			X	
Department Uniformed Personnel			X		X	
Department Technology Consultant		X		X		
Management Information Department		X		X		
Civilian Personnel			X		X	
General Public			X			X
Criminal Suspects			X			X

APPENDIX F

COMMITMENT PLANNING CHART

Key Players	No Commitment	Let it Happen	Help it Happen	Make it Happen
City Council/Board of Supervisors	X —————→ O			
City Manager	X —————→ O			
Chief of Police		X —————→ O		
Department Command Staff		X —————→ O		
California DMV	X —————→ O			
Federal Bureau of Investigation		X —————→ O		
California Department of Justice		X —————→ O		
Department Middle Managers	X —————→ O			
Department Supervisors	X —————→ O			
Department Uniformed Personnel	X —————→ O			
Department Technology Consultant			X —————→ O	
Management Information Department		X —————→ O		
Civilian Personnel	X —————→ O			
General Public	X —————→ O			
Criminal Suspects	O ←———— X			

“X’s” on the Commitment Planning Chart indicate an individual’s current level of commitment to the issue. “O’s” indicate the desired level of commitment needed. The arrows show how much commitment movement is required.

Notes

-
- ¹ Clarke, Roger. "Human Identification in Information Systems: Management Challenges and Public Policy Issues." Information Technology and People. December 1994.
- ² Perez, Juan Carlos. "Microsoft buys biometric security software for Windows." IDG News Service. May 3, 2000. Computer World.
- ³ "About Biometrics." BioLink.
- ⁴ Coleman, Stephen Ph.D. "Solving Cases of Mistaken Identity And More Biometrics." The Journal. Fall 2000. pp. 80-85.
- ⁵ "An Overview of Biometrics." Michigan State University, Department of Computer Science and Engineering.
- ⁶ Phillips, Ken. "Biometric identification looms on landscape of network log-ins." PC Week. March 26, 1997.
- ⁷ Phillips, Ken. "Biometric identification looms on landscape of network log-ins." PC Week. March 26, 1997.
- ⁸ Solomon, Patrick. "A Password You Can't Forget." Government Technology. August 2000: 30-31.
- ⁹ Coleman, Stephen Ph.D. "Solving Cases of Mistaken Identity And More Biometrics." The Journal. Fall 2000. pp. 80-85.
- ¹⁰ Ashbourn, Julian. "The Biometric Whitepaper." ntlworld.com.
- ¹¹ L. A. Times
- ¹² Ashbourn, Julian. "The Biometric Whitepaper." ntlworld.com.
- ¹³ Solomon, Patrick. "A Password You Can't Forget." Government Technology. August 2000: pp.30-31.
- ¹⁴ Ibid.
- ¹⁵ Federal Bureau of Investigation, "Fingerprint Identification" U.S. Government Printing Office. 1986: pp.2.
- ¹⁶ Ibid.
- ¹⁷ Swope, Christopher. "Sherlock Online." Governing. September 2000: pp.80-84.
- ¹⁸ Ibid.
- ¹⁹ Ibid.
- ²⁰ Ruggles, Thomas. "Comparison of Biometric Techniques." The Biometric Consulting Group. March 15, 1998: pp.7-10
- ²¹ Coleman, Stephen Ph.D. "Solving Cases of Mistaken Identity And More Biometrics." The Journal. Fall 2000: pp.80-85.
- ²² "Convenience Vs. Security: How Well Do Biometrics Work?" Recognition Systems □ White Pages.
- ²³ Ibid.
- ²⁴ Coleman, Stephen Ph.D. "Solving Cases of Mistaken Identity And More Biometrics." The Journal. Fall 2000: pp.80-85.
- ²⁵ Phillips, Ken. "Biometric identification looms on landscape of network log-ins." PC Week. March 26, 1997.
- ²⁶ Ibid.

-
- ²⁷ Spence, Bill. "Biometrics in Physical Access Control: Issues, Status, and Trends." Recognition Systems. Internet. Accessed: September 27, 2000.
- ²⁸ Ruggles, Thomas. "Comparison of Biometric Techniques." The Biometric Consulting Group. March 15, 1998.
- ²⁹ Coleman, Stephen Ph.D. "Solving Cases of Mistaken Identity and More Biometrics." The Journal. Fall 2000. pp. 80-85.
- ³⁰ Ruggles, Thomas. "Comparison of Biometric Techniques." The Biometric Consulting Group. March 15, 1998: pp.7-10
- ³¹ Speir, Michelle. "Biometric solutions unveiled at Comdex." Federal Computer Week. November 18, 1999. CNN.Com. Internet. Accessed: April 23, 2001.
- ³² Phillips, Ken. "Biometric identification looms on landscape of network log-ins." PC Week. March 26, 1997.
- ³³ Spence, Bill. "Biometrics in Physical Access Control: Issues, Status, and Trends." Recognition Systems. Internet. Accessed: September 27, 2000.
- ³⁴ Solomon, Patrick. "A Password You Can't Forget." Government Technology. August 2000: pp.30-31.
- ³⁵ Ibid
- ³⁶ Solomon, Patrick. "A Password You Can't Forget." Government Technology. August 2000: pp.30-31.
- ³⁷ Davies, Simon G. "Touching Big Brother: How biometric technology will fuse flesh and machine." Information Technology & People. Vol 7, No. 4, 1994.
- ³⁸ Ibid.
- ³⁹ Ibid.
- ⁴⁰ Clarke, Roger. "Human Identification in Information Systems: Management Challenges and Public Policy Issues." Information Technology and People. December 1994.
- ⁴¹ Phillips, Ken. "Biometric identification looms on landscape of network log-ins." PC Week. March 26, 1997.
- ⁴² Swope, Christopher. "Sherlock Online." Governing. September 2000: pp.80-84.
- ⁴³ Ibid.
- ⁴⁴ Perky
- ⁴⁵ Swope, Christopher. "Sherlock Online." Governing. September 2000: pp.80-84.
- ⁴⁶ Jick, Todd D. "Implementing Change." Harvard Business School. Case #N9-491-114. 1991.pp.192-201
- ⁴⁷ Rogers, Donna, "Making ends meet-Tips for snaring grant money." Law Enforcement Technology. March 2001: pp.36-40
- ⁴⁸ Ibid.
- ⁴⁹ Beer, Michael. "Why Change Programs Don't Produce Change." Harvard Business School Press. 1991. pp.265-276
- ⁵⁰ Kotter, John P., "Leading Change." Harvard Business School Press. 1996: pp.94.
- ⁵¹ Beehard, Richard and Harris, Richard T. Organization Transitions, 2nd Edition. Addison-Wesley, 1987. pp.94-95

⁵² Callahan, David, "Overmatched by Technology." The Washington Post Online. July 22, 2001. pp.B03