

HOW WILL  
BIOMETRIC FACIAL RECOGNITION TECHNOLOGY  
IMPACT THE PREVENTION OF CRIME AND TERRORISM  
IN LARGE, URBAN LAW ENFORCEMENT AGENCIES BY 2008?

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

By

Mike Callagy  
San Mateo Police Department

Command College Class XXXIV

Sacramento, California

October 2003

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 considerations.

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 future study points the way.

The views 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), the San Mateo Police Department, or the city of San Mateo.

Copyright 2003

California Commission on Peace Officer Standards and Training

## TABLE OF CONTENTS

LIST OF TABLES AND FIGURES.....	ii
ACKNOWLEDGMENTS .....	iii
Chapter One – Issue Identification .....	1
Introduction.....	1
Environmental Scanning.....	3
Figure 1.1 .....	3
Figure 1.2 .....	4
Figure 1.3 .....	5
History of Facial Recognition.....	6
How Facial Recognition Systems Work .....	7
Illustration 1.1 - Observation Center .....	10
Figure 1.4 .....	14
Chapter Two – Futures Forecasting Study.....	22
The Nominal Group Technique (NGT) .....	22
Trends .....	24
Table 2.1 - Trends Summary .....	25
Events.....	30
Table 2.2 - Event Analysis.....	31
Cross-Impact Analysis.....	35
Table 2.3 - Cross Impact.....	35
Pessimistic View .....	40
Optimistic View .....	43
Normative View.....	46
Chapter Three – Strategic Plan .....	48
Vision Statement.....	49
External Analysis – The STEEP Model.....	50
Chapter Four – Transition Management .....	66
Introduction.....	66
Chapter Five – Summary, Recommendations and Conclusions.....	74
Summary .....	74
Recommendations.....	75
Conclusion .....	76
Appendix A – List of Nominal Group Participants .....	78
Appendix B – List of Trends .....	79
Appendix C – List of Events.....	81
Endnotes.....	82
Bibliography .....	85

## LIST OF FIGURES, TABLES, AND ILLUSTRATION

Figures	Description	Page
1.1	September-March changes in public's sense of security	3
1.2	Percent of Americans who believe attacks are likely in the near future, by region.	4
1.3	Percent of Americans who say they have become more concerned about doing this activity since September 11, 2002.	5
1.4	Percent supporting specific homeland security measures	14
Tables		
2.1	Trends Summary Table	25
2.2	Event Analysis	31
2.3	Cross-Impact Table	35
Illustration		
1.1	Illustration of Observation Center	10

CHAPTER ONE  
ISSUE IDENTIFICATION

Introduction

Use of biometrics as an identification tool is not new, but the use of facial recognition technology as an identification tool is an emerging technology. This technology has been deployed in limited capacities, yet it is still in its infancy stage in regard to practical applications by law enforcement agencies. Even though long-term capabilities of this technology are unknown, the potential to identify wanted individuals and terrorists before they commit crimes is exciting to law enforcement. This technology, if perfected, may have the ability to save an incredible amount of law enforcement resources while providing unprecedented security to areas where Americans feel most vulnerable.

It is possible that at no other time in history have Americans felt so unsure about their own personal security. “September 11<sup>th</sup> has been a transforming event not just because of the enormity, but also because of the nature of the attacks. Fifty thousand Americans were killed in a decade of fighting in Vietnam. They were combatants dying on battlefields. Over 3,000 people were murdered in one morning in New York, Washington, and Pennsylvania.”<sup>1</sup> For the first time in thirty years, Americans are not safe in their homeland. This has shaken Americans, who, for the most part, came to feel invincible from outside terrorist attacks. Separated by thousands of miles of sea from the nearest enemy, Americans have lived with a false sense of security.

No hostile invaders had dared to attack America since 1812. Walter Russell Mead of the Council on Foreign Relations calls the result a “myth of virtuous isolation.”<sup>2</sup> That fateful September day became a wake-up call of sorts to Americans. No longer could Americans be

assured of security at home. But the question remained as to how Americans would react. Would Americans fight back or would they retreat into their own little worlds? Would the country unite and fight terrorism, or would Americans become isolationists? Would Americans be willing to bend in the one area deemed by most to be the most precious right of all - individual liberties?

It didn't take long to determine which way this great country would go. The September 11, 2001, terrorist attacks rallied Americans and the world like never before. Even perceived enemies of the United States were stunned by the sheer cowardliness of this attack and the loss of innocent lives. Many Americans were lost on that fateful day, but so were many innocent lives representing nations from around the world. The terrorists attempted a surgical strike at the heart of America. That strike destroyed one heart that was quickly replaced by one ten times stronger.

The President of the United States quickly declared war on terrorism, and bombs would soon fall on Afghanistan. The United States, which was easily the most patriotic country in the world,<sup>3</sup> had patriotism go off the charts as the United States led allied troops in a battle that was now brought to the homeland of every American.

Extraordinary times call for extraordinary measures. The United States had clearly and decisively won the battle against terror in Afghanistan, but this was just one battle in an ongoing war with no end in sight.

What remains to be seen is how Americans will adjust to this ongoing war and what expectations they will have in the area of personal security, as well as what liberties they might be willing to relinquish to reach that level of security.

## Environmental Scanning

This lack of security was not just a moment in time, but rather a noticeably systemic occurrence increasingly getting worse. Americans thought that with all the intelligence, with all the police, with all the screening processes in place, America was safe.

The September 11, 2001, terrorist attacks came like a blow from a hammer to the heads of most Americans. How could so much go so wrong so fast? One day, Americans woke up to a different country than when they went to sleep the night before. The United States was no longer safe from catastrophic attacks by terrorists. The question that remained was what the long-term impact would be on law enforcement and the public as a result of that unforgettable day in September 2001. Americans were and remain scared, and this may be a strong signal that the timing is right for new security technology to help fill the void in America's confidence in regard to the security of this nation.

The University of Michigan Institute for Social Research (ISR) polled 613 Americans in March 2002 in regard to their relative feelings of security in light of the September 11, 2001, terrorist attacks. According to a study, 11% of the 613 Americans surveyed were more shaken in May 2002 by the terrorist attacks, 13% said they were less shaken, while 75% said their sense of insecurity was unchanged (see figure 1.1) <sup>4</sup>

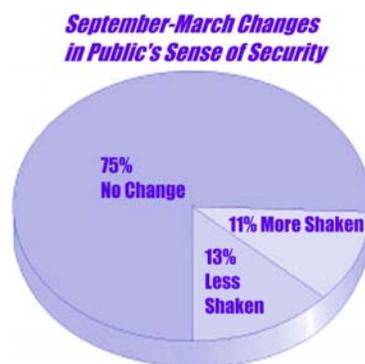
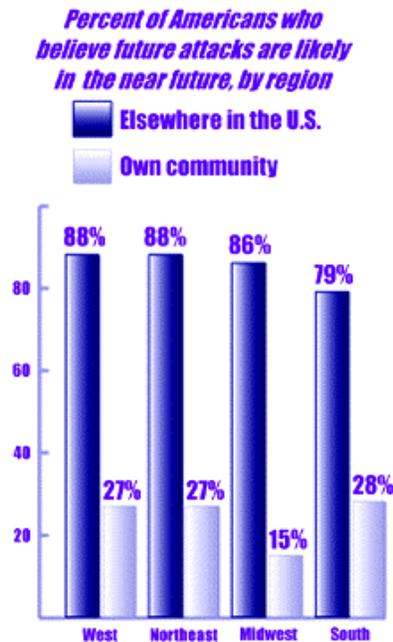


Figure 1.1

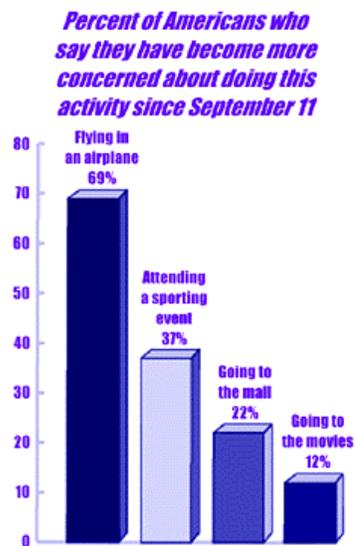
The findings from this survey suggest that the psychological, social, and political effects of the September 2001 events have been profound and enduring. “Despite attempts by the government to assure Americans that homeland security is a priority, most Americans don’t feel any safer today than they did right after the attacks.”<sup>5</sup>

The Michigan ISR study showed that an overwhelming number of Americans polled (84%) felt that it was likely or very likely that another terrorist attack in the United States would take place in the near future.<sup>6</sup> Women are more likely than men to remain shaken by the terrorist attacks; twice as many women reported that their feeling of personal security has been profoundly impacted.<sup>7</sup> More and more Americans are feeling that terrorism represents a real threat to the United States, as well as their personal safety or safety of their family.



**Figure 1.2**

The ISR research went even further to try to establish when Americans feel most vulnerable to terrorism. The results in Figure 1.3 show that most Americans feel vulnerable to terrorism when flying, attending sporting events, or going to the mall.<sup>8</sup> Figure 1.3 illustrates that sixty-nine percent of Americans say they are more concerned about flying now than before the September 11, 2001, terrorist attacks. Thirty seven percent are more concerned about sporting events, twenty-two percent are more concerned about going to the mall, and twelve percent are more concerned about going to the movies. This tends to substantiate the point that the physiological impact of terror may be worse than the reality.



**Figure 1.3**

Biometric facial recognition is most effective when it is used in controlled settings, which may be found or created in malls or other environments. The very fact that Americans are looking for more security in these given areas may expedite the use of this emerging technology.

## History of Facial Recognition

Biometrics is defined as the “automated methods of identifying or authenticating the identity of a living person.”<sup>9</sup> In its purest sense, before automation, biometric identification can be traced as far back as 1879. At the age of twenty-six, Alphonse Bertillon joined the Paris Police Department as a clerk. According to Clive Reedman, author of “Biometrics and Law Enforcement”, young Alphonse was the son of an anthropologist who had spent a large portion of his career attempting to prove that no two human beings possessed the identical physical characteristics and that the distinct characteristics were in fact measurable.<sup>10</sup> Mr. Bertillon somehow convinced the French authorities to allow him to put his father’s theories to a test on prisoners in the French jails.

Mr. Bertillon’s experiment was a success, and he was able to identify hundreds of prisoners in three years. By 1892, he was well recognized for his contribution to law enforcement and was named as the First Director of the Paris Bureau of Identification. He went on to receive the prestigious Chevalier Legion of Honor for his work.

Though Bertillon’s anthropometric system of measurement quickly gained fame, it was not biometrics as it is known today. The thought process was clearly the same, in that Bertillon attempted to identify individuals through distinctive physiological traits. Bertillon would mechanically measure body parts, starting with the cranium, and divide them into sub-groups. Though Bertillon started with only eleven measurements, eventually his system was adopted and modified by others until there were over one hundred points of measurement.

Bertillon’s system was time-consuming and tedious work that began to generate skepticism in the late 1800s. By the early 1900s, England’s Scotland Yard, in search of a more

reliable mechanism for identification, developed the fingerprint branch utilizing a methodology for classification of fingerprints.<sup>11</sup>

The Bertillon system soon died as fingerprints became more reliable, yet the young Frenchman provided a very valuable start to a process that lacked exact measurements and automation.<sup>12</sup> The quality control that was missing in the Bertillon model would be greatly enhanced by advanced emerging software that has been developed over the last several decades.

Though facial recognition software has been around since the 1980s, it has been used only recently on the commercial market. With increasing violent crime rates and the threat of terrorism after September 11, 2001, biometric facial recognition technology has been thrust into the spotlight.

### How Facial Recognition Systems Work

Facial recognition falls into a larger group of technology known as biometrics. This technology uses biological data to verify identity. Faces are a very important part of who humans are and how humans are recognized. The most basic idea about biometrics is that every human body possesses unique properties that can be distinguished from others. Besides facial recognition, other examples of biometrics include, but are not limited to: fingerprint scans, retina scans, and voice identification.<sup>13</sup>

Facial recognition is something that every human being uses on a daily basis. It is already used by humans to recognize friends and foes. As a human walks down the street, the eyes act as sensors sending a message to the brain, which acts as a computer with stored images. As the eyes focus on a face, a message is sent to our brain that retrieves a stored image and identifies it. This simplistic example underscores the basic principles of biometric facial

recognition systems. It can be said that faces are a human's most unique physical trait.<sup>14</sup>

Starting with that premise, it can be easily understood why companies would want to use the physical characteristics of the face to identify an individual who may harm or pose a threat to society.

“Generally speaking, the system works by first obtaining the image of a person. This is usually accomplished by the use of a video camera with at least 320x240 resolution at 3-5 frames per second.”<sup>15</sup> Obviously, a higher-quality camera will produce better results. Facial recognition systems may vary, but the steps usually include capturing a face, analyzing the face, and comparing it to facial images stored in a database.

When recognition software is connected to a video surveillance system, it will search a given field of view for faces. The system can detect a face within a fraction of a second and a multi-scale algorithm (program that provides instruction to do a certain task) is used in situations of low or varied light.

Once a face is detected, an alignment takes place. An individual's head position, along with size and pose, is noted. For most facial recognition systems, the individual's face needs to be turned at least 35 degrees in the direction of the camera. Normalization takes place as the face is mapped and registered into a standardized pose. In this process, light is not a factor. The software then translates the collected data into a unique code. This unique code will allow for a comparison against stored data. The acquired data is then compared against that of the stored data in the effort to make a match.<sup>16</sup>

The four main methods of capturing the needed information are: (1) Eigenfaces, (2) Feature Analysis, or Local Feature Analysis, (3) Neutral Network, and (4) Automatic Face Processing.<sup>17</sup>

Eigenfaces was developed at MIT and is a tool that extracts characteristics through the use of two-dimensional grayscale imagery. This technology, used by many leading companies today, uses a sophisticated algorithm based on Principle Component Analysis that can translate characteristics of a face into a unique set of numbers.<sup>18</sup> There is then a real-time comparison for both identification and verification in an existing database.

Feature Analysis, also called Local Feature Analysis, is one of the most widely used because it can adapt to changes in facial aspects. This is very important in light of criminals or terrorists, who attempt to change facial appearances or features. The Local Feature Analysis uses an algorithm of 84 bytes to create a facial print for comparison.<sup>19</sup>

Neural Network extracts facial features to create a template used against contrasting elements, which is then matched against the existing database. This particular product may be the future of facial recognition.

The last system is the Automatic Face Processing technique that measures distances and ratios between certain facial features.<sup>20</sup> This system is commonly used in poor lighting conditions.

The speed of automation is what makes biometric facial recognition systems such an attractive tool to law enforcement. For example, the Local Feature Analysis can match multiple face prints at a rate of 60 million from memory or 15 million per minute from a hard disk.<sup>21</sup> As the comparisons are made, the system will assign a value of between one and ten. The operators of the system establish a predetermined threshold, and if a score above the threshold is indicated, a match is declared. The operator can then visually compare the match to help determine its validity.

Biometric facial recognition systems could function like many modern-day dispatch centers. Trained staff, who would look for suspicious suspects and direct cameras to capture their photos, would monitor cameras. Or, they would simply monitor the automated process, then verify and authenticate matches made by the automated process. Once a match is made, an observer is able to call police to make an arrest, while the suspect's every move is followed on camera (see Illustration 1.1).



Illustration 1.1

Observation centers, as illustrated above, could obviate the need for more police resources, while providing a better, more reliable, and less expensive way to protect citizens.

### Drawbacks of Biometric Facial Recognition Technology

Biometric facial recognition technology is not without controversy or drawbacks. It is becoming more and more common, yet many see this emerging technology as a governmental intrusion on their right to privacy. Though hardly 100% accurate, and certainly not foolproof,

biometric facial recognition technology is on the fast track to implementation as a promising crime deterrent. In 2001, MIT's *Technology Review* named biometrics, "one of the top ten technologies that will change the world,"<sup>22</sup> yet others, like the American Civil Liberties Union (ACLU), characterize facial recognition as big brother taking society one step closer to a full-fledged surveillance society.<sup>23</sup>

Is it possible that data trails are likely to give government the opportunity to recreate one's activities with such detail that it would be like being followed with a camera twenty-four hours a day? The ACLU seems to believe that this is exactly what the government will be able to do if not stopped.

According to the ACLU, the biggest threat to privacy comes from the government.<sup>24</sup> The ACLU attributes this statement to several factors that include expansive government databases, communications surveillance (including the FBI's new Carnivore program), the Patriot Act (which overnight changed the United States surveillance laws), and the loosened domestic spying regulations.<sup>25</sup>

Critics of government surveillance are not so worried about where it stands today, but rather where it is headed tomorrow. Furthermore, they say that the enormous amount of information collected on Americans is somewhat protected, i.e. it exists in many different databases that do not communicate with each other. Says the ACLU, "The real threat to privacy will come when the government, landlords, employers, or other powerful forces gain the ability to draw together all this information."<sup>26</sup>

Some see the well-intentioned attempt to preserve American security as a slippery slope that could someday lead from specific surveillance to general surveillance and then morph into a

national ID card system. Government officials argue that facial recognition systems will add another layer of security, but will not undercut civil liberties.<sup>27</sup>

The question remains as to how far facial recognition systems will be able to go before they are considered an invasion of privacy, but it seems that they will remain legal for now. In Richmond, Virginia, a bill was introduced that would have required a judge's signature to deploy facial recognition; however, an 11-4 Senate panel vote shelved deployment. Currently, there are no standard guidelines for the use of biometric facial recognition surveillance, leading some lawmakers to feel that the databases are on the verge of an explosion.<sup>28</sup> There has clearly been a proliferation of cameras since September 11, 2001, but are they really an invasion of privacy?

While the human recognition of a face is cognitive in nature, the biometric recognition of a face could be said to be more computerized and automated. Does this mean that it violates Americans' rights to privacy? Starting with the United States Constitution, there is no mention of the word privacy. Yet several amendments of the Constitution, namely, the First, Third, Fourth, Fifth, and Fourteenth, address the concern of government intrusion into the lives of individuals. So, with a closer look at the Constitution, there are implicit physical privacy rights, along with the Supreme Court's espoused concern with the "accumulation of vast amounts of personal information in computerized data banks or massive government files."<sup>29</sup>

While some civil libertarians might argue that the massive dragnet that takes place on busy weekends in Ybor City, Florida, or during the Super Bowl in Tampa is improper and in violation of individuals' Fourth Amendment Right against illegal search and seizures, the above searches are surely constitutional.<sup>30</sup> The Court has consistently found that an individual does not have a privacy expectation to personal physical characteristics that are constantly exposed to the public, like facial features.<sup>31</sup>

John Woodward, Jr., of Rand foresees that as facial recognition systems become interlinked, the threat to information privacy increases.<sup>32</sup> If systems become superlinked, governments could potentially trace the movements of any individual recorded in the database. This would presume the widespread proliferation of cameras that would potentially capture images on the freeway, on the subway, at the ATM, about town, and even in the cleaners!

Once an individual is in the system, Woodward goes on to suggest that the possibility exists for government to link information on an individual's friends. The friends might then be placed on a watch list, and government could reverse engineer the friends' identities in order to track their whereabouts for the last several months.<sup>33</sup> Yet, the only real way that even this super surveillance may be found to be unconstitutional is if it had a chilling effect on an individual's ability to attend First-Amendment protected activities.<sup>34</sup> This is unlikely to be found true, but only time will tell if and when databases are in fact connected in the future.

What has clearly been found to be the case, especially in light of September 11, 2001, is that Americans seem ready to give up some civil liberties in order to secure their safety. In one study by the University of Michigan ISR, after September 11, 2001, and in March 2002, over 70% of individuals polled said they would be willing to give up some of their civil liberties to ensure more homeland security.<sup>35</sup> As noted in figure 1.4, this research also revealed that most Americans would support increasing homeland security measures.<sup>36</sup>

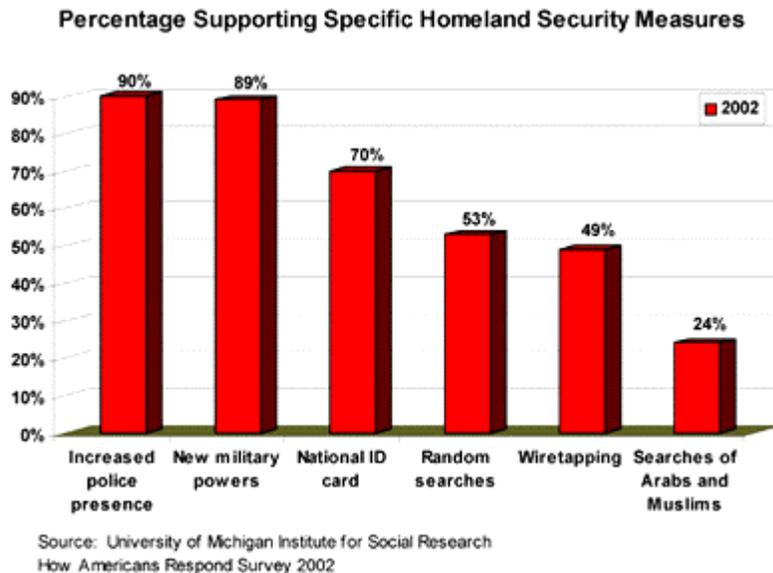


Figure 1.4

The other major complaint that libertarians have espoused against law enforcement's use of biometric facial technology is that it is not a proven tool in increasing safety and that it is inaccurate. A pilot program by the Department of Defense tested facial recognition technology. Using 270 subjects, the Defense Department found a 51% accuracy rate and an 81% accuracy rate in narrowing the field to ten.<sup>37</sup> Past tests at the Palm Beach Airport in Florida have caused the ACLU to have grave concerns about the inaccuracy of facial recognition technology.<sup>38</sup> Additionally, tests at Logan Airport in Boston have also shown how inaccurate the new technology can be.<sup>39</sup> The equipment also performs poorly in varied lighting conditions and with varied backgrounds.

Some argue that allowing invasion of privacy during heightened times of stress, when safety is a concern, is a natural reaction, albeit an overreaction.<sup>40</sup> Jeffery Rosne, an author and attorney, thinks that this technology may offer frightened citizens a false sense of peace of mind, which certainly won't accomplish the goal of preventing terrorism. Rosne feels that the terrorists

likely to do harm are unknown individuals; if they were known, we would simply go out and get them.<sup>41</sup>

This emerging technology undergoes government scrutiny through face recognition vendor tests (FRVT). These tests are independent government evaluations of commercial facial recognition software, which is currently available. The tests are specifically designed to provide the U.S. and law enforcement independent evaluations of which products work and how they can best be used.<sup>42</sup> The 2002 test results are pending and will be closely scrutinized by both government and civil libertarians.

#### Benefits of Biometric Facial Recognition Technology

The emerging technology of biometric facial recognition must be explored because of the potential it has for preventing crime and capturing terrorists. Crime has been on the rise in recent years and promises to get worse before it gets better. In the first nine months of 2002, the California Crime Index (which tracks homicide, forcible rape, robbery, aggravated assault, burglary, and motor vehicle theft) showed a 5.3% increase.<sup>43</sup> Most surprising is that homicide was up 13.1%; forcible rape was up 2.6%, and robbery was up 4.5%.<sup>44</sup>

Terrorism is likewise on the rise. In 1996, in Saudi Arabia, a terrorist truck bomb exploded killing 19 servicemen. In the following years, truck bombs in Kenya killed 224 and wounded 4,600 others. Later in Yemen, the USS Cole was attacked killing 17 sailors and wounding 42 more. Then, on September 11, 2001, the United States changed forever when over 3,000 were murdered in the worst terrorist attack in history.

The threat of continued terrorism and crime in the homeland is a real one. Federal and local law enforcement agencies need as many tools as possible to separate the good guys from

the bad guys and try to prevent criminal acts before they occur. As it stands now, there are millions of cameras all over the United States, but there is no one centralized database or way to classify or sort these images. Criminals are caught on tape everyday, yet they continue to go unpunished because police are frustrated by a lack of ability to identify them.

One of the most unforgettable and haunting images of the September 11, 2001, terrorist massacre was that of the face of hijacker Mohamed Atta as he walked past a metal detector in the Portland, Maine, airport. Could the terrorist attacks of September 11, 2001, have been stopped if a biometric facial recognition system was in place at the Portland airport? That question will never be able to be answered because there was no system in place. Federal and local law enforcement officers are at a distinct disadvantage in this highly mobile and transient-oriented society. Police are constantly caught in a game of here today and gone tomorrow.

Typically, in a large urban law enforcement agency, officers will respond to the scene of a crime, where the image of the suspect has been captured on closed circuit television (CCTV) or some digital surveillance camera system. Officers will look at the image to determine if they know who the person is from past encounters, or they may sift through thousands of in-house photos in an effort to identify the suspect. Officers may also send out technology to recover abducted kids (TRAK) flyers with the suspect's image and a brief synopsis of the crime to all local law enforcement agencies. When they become completely frustrated, they may forward the photo to the print media or news agencies for distribution. But unless these cases are high profile or somehow newsworthy, the police will never get the necessary help from the public that may lead to the identity of the suspect. Police spend countless frustrating hours looking to identify the suspect in the image, yet the end result is usually that another suspect goes free to victimize again.

Biometric facial recognition technology promises to be the tool that acts to level the playing field. The beauty of this system is that it is so convenient and not intrusive. At the Super Bowl in 2001, over 80,000 fans passed through the system and didn't even know it. Bill Todd, a detective with the Tampa Police Department, who was responsible for crime prevention at the Super Bowl said, "The facial recognition technology is an extremely fast, technologically-advanced version of placing a cop on a corner, giving him a face book of criminals and saying, 'Pick the criminals out of the crowd and detain them.' It's just very fast and accurate."<sup>45</sup>

Though Super Bowl XXXV may have been the first location where biometric facial recognition was used at a major sporting event, it is by no means the only place that it can be used. From airports to every location where there is the potential for crime or a terrorist attack, this technology can be deployed. In fact, one of the first uses of this technology by law enforcement in New York City was at the Statue of Liberty. David Barna, Chief of Public Affairs for the National Park Service, called the technology, "A cost-effective means of improving security at the statue."<sup>46</sup>

The list of possibilities goes on to include check cashing and credit card security, which, due to the mounting cases of identity theft, are major concerns throughout the United States. Beyond surveillance, facial recognition systems promise to be big security items in personal computers, the department of motor vehicles, security door companies, and automated tellers. Biometric facial recognition systems may also someday help to reduce auto theft. The possibilities are endless. You may someday see this same system in stores as a way to expedite customers through lines while automatically billing them.

Even Rand, who has historically been the arbitrator of controversial issues and rarely takes sides, sees the benefits of facial recognition. Biometric facial recognition systems are

described as a tool that can provide significant benefits to society.<sup>47</sup> There is no doubt that this technology must be balanced against the privacy concerns of the public, but it has the potential to be a very powerful law enforcement tool that is less intrusive than a fingerprint scan. Society as a whole must decide how to harness the extreme power of this tool, while ensuring that individual freedoms are not completely trampled in the process.

### The Future of Biometric Facial Recognition

After the 1996 Kobar Towers terrorist attacks, the Defense Advanced Research Projects Agency (DARPA) started a \$50 million program that was known as the “Human ID at a Distance.” The group’s goal is to help develop biometric technologies like facial recognition that can be used to identify known terrorists at a distance before they attack. This effort has the promising goal of saving lives.<sup>48</sup> Additionally, the next phase of biometric facial recognition will be the development of a system that is not so sensitive to light conditions. One of the major drawbacks of biometric facial recognition systems is that they work best under controlled lighting and background conditions. Since lighting and background cannot always be controlled, more advanced technology will lead to systems that can better adjust to these conditions, while getting a more accurate 3-D facial image than current systems. These future systems are promising because of their potential widespread application.

In the future, it is possible that all law enforcement agencies will be using some form of facial recognition system. One of the many tools that the Huntington Beach Police Department currently uses is the Imagis Computer Arrest and Booking System (CABS) ID 2000, which uses facial recognition technology.<sup>49</sup> The Huntington Beach PD uses the CABS system not only to expedite booking, but also to encode scars, marks, and tattoos. The other real advantage of

CABS is that it will allow encoding of a suspect's photo from a security video, and, if a prior booking photo is in the system, CABS could help to identify the suspect in the video through facial recognition.<sup>50</sup> Additionally, the system can be used to create photo lineups based on similar facial features. Work is in progress to allow Huntington Beach PD to exchange information with other agencies that will ultimately move to increase their database from 45,000 images to over half a million.<sup>51</sup>

Some other promising uses of facial recognition are in the area of identification of wanted individuals. The city of Los Angeles has tens of thousands of outstanding wanted individuals who continue to victimize innocent citizens. The Los Angeles Police Department is in the process of developing a facial recognition system with images of all wanted individuals in the database. The Los Angeles police will then be able to set up surveillance in known narcotics locations, in disorderly areas at public events and at transportation hubs in an effort to locate wanted individuals through facial recognition technology.<sup>52</sup> This could have a profound and long-lasting impact on Los Angeles' crime rate and could act to prevent thousands of crimes by taking known criminals off the streets.

If this technology keeps evolving, there is a strong likelihood that officers in the future will have the capability to identify suspects in the field with handheld devices that could be as small as PDAs. If biometric facial recognition is not explored to its full potential, local law enforcement may have to live with the prospect of a disaster that could have been prevented.

### Project Outcome

The goal of this project is to forecast how biometric facial recognition technology will prevent crime and terrorism in large urban law enforcement agencies by the year 2008. The

outcome of this project should be the identification of the issues, opportunities, and obstacles that may hinder the achievement of that goal, along with the development of fiscally responsible and practical first steps to achieve that goal. The initial steps, such as the ones taken by the city of Los Angeles and other cities discussed above, can be taken today. The steps should be monitored and adjusted as needed to address the issues that will impact law enforcement's ability to safely protect the public by the year 2008. Readers should not expect this emerging technology to be the silver bullet that will provide a comprehensive blanket of protection to the homeland. This project must be viewed as an emerging issue that will act as a tool in law enforcement's arsenal to fight the violent war against increasing crime and the threat of terrorism.

### Summary

Despite the fact that Americans hold privacy from governmental intrusion as one of their fundamental rights, the threat of terrorism and the rising crime rate has dictated that law enforcement be given more tools to keep Americans safe. To assist officers in the identification of wanted or dangerous individuals and to safeguard the homeland from known terrorists, the emerging technology of biometric facial recognition must be developed to its fullest capacity and logically deployed.

Chapter 1 focuses on what biometric facial recognition is and how it can prevent crime and terrorism. The trend of trying to protect Americans through the use of biometrics is likely to continue at an exponential rate. Using environmental scanning, literature review, interviews, an investigation of potential problems and advantages to this technology, along with future

projections of this issue, a well-rounded exploration of the entire subject has been presented in this chapter.

The following chapter will present an analysis of various trends and events that may significantly impact this issue. Also explored is how the trends and events may impact each other, and then a look at some possible future scenarios will be investigated.

## CHAPTER TWO

### FUTURES FORECASTING

Futures study is used to project the future and influence positive change. By using future forecasting, certain actions can be taken to help bring about a desired change, while helping to avoid negative consequences of change. Future forecasting is a holistic approach to the future, so that can be used to anticipate, participate in, and help influence change to bring about desired results.

One of the many tools often used in any group process is the Nominal Group Technique (NGT). When used for future forecasting, trends and events of a particular topic can be examined, and a cross-impact analysis can be developed to help determine how those trends or events will influence the issue. Following that in-depth analysis, future scenarios (positive, negative, and neutral) are developed, which relate to the use of biometric facial recognition technology in public places by law enforcement officers.

#### The Nominal Group Technique (NGT)

The NGT is a structured workshop/process that identifies and ranks major trends and events related to a particular issue. The NGT is usually held in a casual setting, which promotes creative and individual thinking. The process works best when facilitated by an independent third party. The process can also be used for planning, measurements, and performance improvement. The method is effective at gaining consensus with all types and levels of participants in a wide range of settings. The exercise is a simple and effective way of getting a group to take a comprehensive look at a particular issue.

It is extremely important to get a diverse group with some knowledge of the issue at hand who are independent thinkers, yet will work to build a consensus on various thoughts. The structure of the NGT works to ensure maximum participation by all members of the group and seeks to avoid the detrimental impact of a strong personality type, who may try to steer the outcome(s) in one direction. The structure of the NGT is such that all participants are given equal input so that they will have an equal opportunity to influence the outcome(s) on the issues that the group will collectively develop.

The NGT process includes four steps: silent reflection and thought, where ideas are generated; a round-robin recording of those ideas; discussion/clarification of the generated ideas; and, then, the ranking of the ideas.

Great thought was given to the selection of NGT participants for this research, so to end up with a diverse perspective on the issue of biometric facial recognition (BFR) technology by law enforcement. The panel consisted of a chief executive officer from a security technology company; two senior management analysts with varied backgrounds; the director of a security-based technology company, who is also a retired FBI agent; an assistant city attorney with an extensive background in civil rights issues; a retired police captain who has worked on security issues for police; and a police sergeant with a background in facilities security (see Appendix A).

Each panel member was contacted personally and provided with a brief overview of Command College and future forecasting. In addition, they were sent extensive written documentation on the issue, how the NGT process works, and a description of trends and events. This documentation also included information on how the trends and events data would be used to prepare a cross-impact analysis.

Once the participants arrived for the NGT, they were informed as a group how the process would work and what their expected roles were. The group was asked to share both trends and events that might influence how the use of biometric facial recognition technology by law enforcement may impact the prevention of crime and terrorism in large, urban law enforcement agencies by 2008.

After the silent generation of thoughts period, the participants shared in a round-robin fashion until all ideas were exhausted. The group generated twenty-eight (28) trends and nineteen (19) events, which they identified as important and material issues. After a lengthy discussion, which at times was heated, the group discarded some of the ideas, incorporated others, and ranked the trends and events, eventually narrowing to the top eight events and top nine trends. After more discussion, again sometimes heated because of different perspectives, the group reviewed all the trends and events until each member of the panel fully understood which ones were to be explored (see Appendices B and C).

### Trends

Trends are defined as a series of incidents or events taking place, which seem to indicate a direction in which a particular issue may be heading. It is based on the past, present, and future and can be quantitative or qualitative. Examples of trends could be changing demographics, educational opportunities, or future technology. Trends should be simple observations. They should be specific, but not complex. NGT panelists were asked to be creative and think unconventionally.

The panel estimated the levels of each trend at various places in time and assigned a level of concern to the top nine trends. Table 2.1, column 3, labeled as “Today” indicates the level of

the trend in question at present day. The value of 100 is an arbitrary value that simply indicates the current level of the trend. The purpose of this exercise is to rate the level of the trend in question five years in the past and five and ten years into the future. The participants project out based on their opinion as to where the trend has been and where it is going to go within the time frames indicated.

The last column titled “Concern 1-10” is an indication of the participants’ opinion of their level of concern regarding the trend’s impact on the issue in the future. A “10” signifies a great deal of concern about a trend, while a value of “1” indicates little concern. The value of identifying those trends that the group is concerned with the most can help focus efforts on either promoting the continuance of a trend or attempting to thwart the advance of a trend if it is within the power to do so. Table 2.1 represents information about trends collected by the NGT panel.

Trend Summary Table

Trends	-5 Years	Today	+5 Years	+10 Years	Concern 1-10
T1 Level of public privacy expectations	137	100	67	50	5
T2 Number of cameras in public places	46	100	150	240	8
T3 Level of concern for homeland security initiatives	38	100	170	150	7
T4 Video surveillance moving from reactive to proactive	10	100	200	250	9
T5 Level of technology in relation to legal constraints	90	100	117	103	3
T6 Level of commitment to develop biometric facial recognition standards	7	100	114	124	8
T7 Amount of lawyers questioning validity of biometric facial recognition	147	100	84	75	5
T8 Amount of suicide/homicide bombings	40	100	143	149	5
T9 Level of accuracy of facial recognition technology	38	100	142	174	7

Table 2.1

The panel median consensus on these nine identified trends is discussed below.

#### Trend 1: Level of public privacy expectations

The NGT panel believed that the terrorist attacks in New York have had a dramatic impact on citizens' level of public privacy expectations. The group talked about the overall feeling that society has been willing to give up some public privacy expectations in return for a sense of safety and security. It was interesting to note that the group felt that within five years the level of public privacy expectations would decrease dramatically and then decrease even more between years five and ten. According to the group, this would be due to the strong sense that terrorist attacks will become more prevalent over the next ten years, and, as a result, more people will be willing to give up freedoms that they once enjoyed. The group believed that the lowering of privacy expectations would have a profound impact on the technological development and implementation of surveillance cameras in public places.

#### Trend 2: Number of surveillance cameras in public places

The NGT panel believed that there is a growing amount of cameras in public places. The group talked about the proliferation of cameras as a means of watching people in various settings such as airports, sports facilities, and at city, state, and federal facilities. The group believed that there would be a dramatic increase in the amount of cameras in public places between years five and ten due to the panel's expectation that homeland terrorism will be more prevalent. The panel also expected more and more people to accept this trend, as cameras become smaller and more aesthetically appealing. The group indicated that this trend would be of great concern in that it

would have a significant impact on the future, as it is a direct reflection of citizens' willingness to give up privacy rights.

#### Trend 3: The public's level of concern for homeland security initiatives

The NGT group felt that five years ago there was little outward concern for homeland security initiatives, but in the next five years that level of concern will significantly increase from where it is today. That, in part, is due to the fact that most NGT participants felt there is a strong likelihood of future terrorist attacks in the United States. From the voting, it appeared the concern would be relatively short and within ten years the concern would still be higher than it is today, but less than it was five years from now. There was a belief by the group that the United States could be victimized for a short period of time, but that the United States would take action to ensure that it would not be victimized on a sustained basis. Again, the NGT group felt the impact of this trend would have a profound impact on the development and implementation of surveillance technology in public places.

#### Trend 4: Video surveillance moving from reactive to proactive

The group said that, for the most part, video surveillance systems have been reactive in that they tend to capture crime instead of actively preventing it. The NGT group felt that as a result of terrorist threats and reports of future attacks, there is currently a trend in making surveillance more proactive. The NGT group sees the trend as one where experts will pick out suspicious activity and then call security or police to investigate the actions of the person before the anticipated crime is committed. It is the group's belief that proactive surveillance is going on all across the United States as a result of heightened awareness of security concerns. The group

saw this as a major impact on the future of video surveillance technology. They also felt there could be a possible impact on crime and terrorism because of the opportunity to make suspects feel like they are being watched before they have a chance to commit a crime.

#### Trend 5: Level of advancements in technology in relation to legal constraints

The NGT group noted a strong trend in the advancement of technology, but that technology was ahead of legal constraints. It is interesting to note that the group saw the exponential growth of technology surpassing legal restraints that are now in place. The group opined that the law will be constantly struggling to keep up with the proliferation of technology in that technology keeps pushing the outer limits of what is legal. What is interesting is that the group saw the trend level increase from 100 to 117 by year five, then a decrease between years five and ten. This is mainly due to the fact that one person in the group thought that there would be a significant drop in technological advances between years five and ten, thus allowing the legal constraints to catch up to the technology. The group did not place a great level of concern on this trend because they indicated that this is typically how the legal system works. In other words the system does not anticipate changes; instead, it reacts to them.

#### Trend 6: Level of commitment by the us government to develop BFR standards

The NGT group had an interesting discussion on this trend. The group felt that, prior to the terrorist attacks in the United States, there was very little interest by state, federal, or local government to develop biometric facial recognition standards because the system was not really being used. The group felt that there would be significant growth in this field because of the government's obligation to make citizens feel safe. They felt that as facial recognition systems

are utilized more readily, there would be the need to create standards in regard to what is considered a match and when that match could be used to detain or arrest an individual. The group felt that this trend by the government to develop standards for biometric facial recognition would grow over the next ten years and that it would be a high concern.

#### Trend 7: Number of lawyers questioning validity of BFR

The group felt that the level of scrutiny by lawyers as to the validity of biometric facial recognition systems has significantly decreased over the last five years and will continue to decrease over the next ten years. The group felt there were three significant reasons that contributed to the decrease in validity to challenges. The first was that the terrorist attacks have led to new privacy laws and expectations, and because of the necessity to protect the public, courts were not likely to invalidate the accuracy of this technology. Secondly, the technology is dramatically improving, and thirdly, this is an investigative tool and not likely to result in significant deprivation of constitutional rights that govern illegal search and seizure.

#### Trend 8: Number of suicide/homicide bombings in the United States

The NGT group engaged in significant discussion about whether a terrorist attack, when an individual explodes himself in a public place with the intent to kill others, is considered a suicide or homicide bombing. For the purpose of this discussion, the terms were deemed to be synonymous. The group decided that five years ago this type of action was relatively low, but the group saw a definite increase in this activity over the next ten years as terrorists try to strike fear in Americans. The group felt that this was of moderate concern because of the increase in security measures around the United States.

## Trend 9: Level of concern regarding accuracy of BFR technology

The NGT group felt there was significantly less concern over the accuracy of facial recognition technology in the past, but that over the next ten years it will greatly increase. The group did not see this as a concern for legal reasons, but rather out of a necessity to protect the public. The group felt that there would be tremendous pressure to put systems in place that will recognize terrorists or criminals and stop them before they commit a crime. They rated this particular trend with a rather high-level concern.

## Events

Events are different from trends in that events are singular occurrences that transpire at a specific time and date. For example, an earthquake, the terrorist attacks on September 11, 2001, or a devastating fire on a certain date are all considered events. The passage of a new law that would mandate a certain action is an event. The types of events solicited were possible future events, positive or negative, regarding how biometric facial recognition technology would impact the prevention of crime and terrorism in large, urban law enforcement agencies.

In Table 2.2, the panel rated the impact of the top eight events and whether the impact would be positive or negative on the topic. The first column designated “yr > 0” was their estimate of when (the number of years into the future) the event in question could first occur. The second column designated “+5 yrs” indicates the probability of an event occurring within the next five years. This value is registered as a percentage. The third column designated “+10 years” indicates the probability of an event occurring within the next ten years. The last column designated “Impact +5 to -5” indicates the level of impact that an event would have on the issue in question and whether or not that impact would be considered positive or negative.

There is no science to these estimates. There are no right or wrong answers. Each participant was asked to make their own estimate or guess based upon their knowledge and experience.

Using the median, all of these ratings took place after the group agreed on the top events to be rated.

Event Analysis Table

Event	Year >0	+5 Years	+10 Years	Impact (-10 to +10)
E1 Restrictive court decision on biometric facial recognition systems in public places	5 Years	36%	50%	-6
E2 Next major terrorist attack in the United States	3 Years	88%	97%	+8
E3 Facial recognition fails to prevent terrorism attack	2 Years	80%	93%	-1
E4 Major wanted criminal identified by biometric facial recognition system	5 Years	78%	96%	+6
E5 National ID System Instituted	4 Years	31%	50%	+9
E6 First major lawsuit due to failure of facial recognition system	5 Years	76%	80%	-4
E7 First wrongful arrest due to facial recognition technology	2 Years	73%	87%	-7
E8 Supreme Court decision decides no expectation of privacy in regard to facial recognition	4 Years	53%	61%	+10

Table 2.2

Discussed below is the panel consensus on these eight identified events.

Event 1: Restrictive court decision on biometric facial recognition systems in public places

The NGT group had an interesting discussion on this particular event. Some group members, who place a strong value on individual freedoms, intimated that they viewed this as a

positive event. It was interesting in that there was almost uniformity in the group's belief that the government would go too far with the impingement of individuals' rights thus prompting a restrictive court decision. In fact, the group believed that within ten years there was a 61% chance that a restrictive court decision regarding the use of biometric facial recognition of individuals in public places would come to fruition. The group noted that if the court did issue a negative ruling on use of BFR, it would have a significant negative impact on the issue being discussed.

#### Event 2: Next major terrorist attack in the United States

It was apparent to the NGT group that this question was not one of "if," but rather of "when." The group thought that within three years there would be a major terrorist attack in the United States. The probability grew to almost 100% certainty within the next ten years. Though this would be a tragic event for Americans, the NGT group saw this as a very positive impact on future innovative security technology. The group felt that another random attack in the United States would further erode citizens' desire to clutch individual freedoms at the risk of losing their own security. The group felt that there would be a rush to develop security technology, and biometric facial recognition would be part of that rush.

#### Event 3: Facial recognition fails to prevent terrorism attack

The NGT group was split on this. Some in the group thought that this situation would result in a devastating blow to biometric facial recognition technology. Others in the group thought more money would be put into research to develop a more accurate system.

The group indicated that this could happen within two years; the likelihood would then go up in five years and continue to rise within ten years. The group discussed the fact that no system is perfect and that someone is bound to slip through the cracks. This should only have a mild negative impact. It is believed that through the inevitable investigations that would follow such an event, information would be developed on how to improve the system. The analogy to planes was made: Just because they crash, we don't stop using them; we make them safer.

Event 4: Major wanted criminal identified by biometric facial recognition system

The group thought if a major wanted criminal, such as a murderer or terrorist, was identified and captured due to a facial recognition system, it would have a positive impact on the issue. The group felt confident that an important identification would take place within the next five years, and the likelihood of that event occurring within the next ten years was almost 100%. They felt that if this event did occur, it could act to prevent terrorists from coming to this country or it could prevent criminal conduct. It is believed that this would act as a tremendous boost to national security and relieve some feelings that terrorists are everywhere.

Event 5: National identification system instituted

The group felt that a national identification system could be instituted within four years, but that there are all kinds of constitutional issues surrounding this proposition. The question the group kept asking was, "what if you don't register?" The group indicated that this issue is so complicated, there was only a 50% chance of it coming to fruition in the next ten years. It would have a major impact on the development and implementation of biometric facial recognition

systems. Presumably, everyone would be in the database, and movement could be restricted or watched through the system.

#### Event 6: First major lawsuit due to failure of facial recognition system

The group felt that once biometric facial recognition systems are in place, there would be a heightened sense of security. This would be accompanied by a possible false sense of safety, and if a feeling of safety were violated, a lawsuit would follow. They also felt there was a very real possibility of this occurring within the next five years and an 80% chance within the next ten years. The group felt that such an event would have a rather negative impact on the use of facial recognition systems, as the government might be worried about litigation.

#### Event 7: First wrongful arrest due to facial recognition technology

The group felt that in a matter of two years, some individual could be falsely arrested due to facial recognition technology. The group assumed this in part due to the current lack of standards associated with the technology and the belief that the technology will never be 100% accurate. They also felt that, due to terrorist attacks, there could be pressure to get these systems in place. The group noted there was almost a 90% chance that in ten years an individual could be falsely arrested due to facial recognition technology. Such an arrest could have a significant negative impact on the issue.

#### Event 8: Supreme court decides no expectation of privacy in regard to facial recognition

The NGT group felt that, within the next four years, the court could reduce individual personal liberties due to terrorist acts and rule in favor of facial recognition technology. The

group noted that, within the next ten years, there would be over a 61% chance of this happening, and, if it did, it would provide the highest positive impact on the subject matter.

Cross-Impact Analysis

Following the NGT process, a cross-impact analysis was completed to project the impact of the events on the various trends, which is recorded as a matrix in Table 2.3. The table represents the top trends and events on a scale of one to five, with five representing the highest impact on the given issue and one representing the lowest impact. The impact is also represented in terms of its positive or negative impact on the topic. The results can be used to identify the trends and events that will likely impact the problem statement in a positive manner, while helping to illuminate the trends and events that could negatively impact the problem statement.

Cross-Impact Table

Events	Trends								
	T1	T2	T3	T4	T5	T6	T7	T8	T9
E1	-5	-4	-1	-4	-3	-4	-2	-5	-3
E2	+4	+5	+5	+5	+2	+5	+2	-3	+3
E3	-1	-4	+4	+2	+3	+4	-3	-4	+3
E4	+4	+4	+3	+5	+2	+4	+1	+3	+4
E5	+2	+4	+3	+4	+2	+2	-1	+3	+3
E6	-3	-1	-3	-4	-4	-3	-4	-3	-3
E7	-3	-3	-1	-4	-3	+4	-2	-2	-2
E8	+4	+5	+4	+4	+1	+1	+3	+1	+2

Table 2.3

The influences that selected events have upon selected trends, where the impact was rated at four or greater upon the problem statement, are discussed below. Panelists’ discussions and specific comments during the NGT process were used to select the following events and trends.

(1) E1- Restrictive court decision on facial recognition systems in public places

T1- Level of public privacy expectations

The cross-impact analysis revealed that event 1 would have a negative 5 impact on trend 1. Interestingly enough, depending on one's perspective, a restrictive court decision would be a positive thing. This was clearly espoused during the NGT. Though some personally view a restrictive court decision as a positive event, it would greatly increase the level of public privacy expectations and have a profound negative impact on the subject matter. The question still remains: What individual liberties are people willing to surrender in the name of privacy? If more privacy rights are granted or protected, it will be much more difficult to place biometric facial recognition systems in public to prevent terrorism or crime.

(2) E2- Next major terrorist attack in the United States

T2- Amount of cameras in public places

The cross-impact analysis revealed that event 2 would have a positive 5 impact on trend 2. Everyone in the group agreed that it was not if, but when, the next terrorist attack would take place in the United States. The group agreed that the event in question would act to increase the amount of cameras in public places. This could expedite the need for more advanced biometric facial recognition systems in an attempt to stop acts of terrorism. It is almost ironic how such a negative event could impact a trend, thus having a great impact on the subject matter.

(3) E3- Facial recognition fails to prevent terrorism attack

T2- Amount of cameras in public places

The results of the cross-impact revealed that event 3 would have a positive 4 impact on trend 2. The analysis suggested that if a facial recognition system fails to prevent a terrorist attack, the amount of cameras in public places will increase, and there will be more of a desire for facial recognition systems to be in place. It seems strange that a negative event could act to advance the problem statement. It was the group's feeling that if another terrorist attack takes place, people will need to feel safe and secure and will be willing to give up more rights for security. To that end, there is a belief that there will be a desire for the implementation and distribution of more cameras after the next terrorist attack. It was strange that the group mostly talked about preventing terrorism as opposed to preventing everyday criminal behavior. There seemed to be a tacit acceptance of crime as it exists today, as opposed to the acceptance of terrorist attacks.

(4) E3- Facial recognition fails to prevent terrorism attack

T6- Level of commitment to develop biometric facial recognition standards

The cross-impact analysis revealed that event 3 would have a positive 4 impact on trend 6. It is believed that if facial recognition systems fail to prevent a terrorist attack, instead of the system being scrapped, more money could actually be put into it to enhance the technology. This would be especially true if the terrorist was in the database and was missed because the technology did not make a match due to lighting conditions, disguises, or based on an outdated photo. The general feeling is this: There is a better chance of identifying a face in a crowd via database than by the human eye.

(5) E4- Major wanted criminal identified by biometric facial recognition system

T4- Video surveillance moving from reactive to proactive

The results of this cross-impact analysis revealed that event 4 would have a positive 5 impact on trend 4. The results suggest that if a major criminal is apprehended because of biometric facial recognition technology, it will have a major positive impact on video surveillance moving from reactive to proactive. This in turn will have a major impact on the subject matter as governments move to pick criminals out of crowds. The group suggested that the current video surveillance is mostly reactive. Simply put, video surveillance tries to capture the crime or deter it by recording it. In the future, it is believed that these systems will become much more proactive as they seek out criminals and attempt to capture them before and shortly after a crime.

(6) E5- National ID system

T4- Video surveillance moving from reactive to proactive

The cross-impact analysis revealed that event 5 would have a positive 4 impact on trend 4. The results suggest that a national ID system would have significant positive impacts on video surveillance moving from reactive to proactive. If there were a database that contained photos of all legitimate citizens, it was felt that the government would be better able to monitor the movement of citizens within the borders. This could cause video surveillance to go from its current reactive state to a more proactive model.

(7) E6- First major lawsuit due to system failure of facial recognition system

T7- Amount of lawyers questioning validity of BFR

The cross-impact analysis revealed that event 6 would have a negative 4 impact on trend 7. It is believed that a profound negative impact from the first failure of a BFR system will result in a large increase of lawyers questioning the validity of biometric facial recognition systems. The group talked about a situation where a suspect was in the database and should have been detected but was not, and he or she went on to commit a major terrorist act or crime in the future. It is believed that lawyers would bring lawsuits following such a failure of the system. The group realized that fear of litigation must be considered when developing advanced technology, especially technology that is in place to save lives.

(8) E7- First wrongful arrest due to facial recognition technology

T6- Level of commitment to develop facial recognition standards

The cross-impact revealed that event 7 would have a positive 4 impact on trend 6. It is believed that the first wrongful arrest due to facial recognition technology will result in an increased level of commitment to develop facial recognition standards. There was much discussion during the NGT about the lack of standards currently regulating the deployment and use of facial recognition technology. It was felt that without these standards, false detention or arrest could become prevalent, which could lead to a negative impact on the subject matter.

(9) E8- Supreme court decides no expectation of privacy in regard to BFR

T1- Level of public privacy expectations

The results of the cross-impact analysis suggest that event 8 would have a positive 4 impact on trend 1. The group felt that if the Supreme Court decides that there is no expectation of privacy in regard to biometric facial recognition, then the level of public privacy expectations

would be greatly diminished. This would be viewed as a profound positive impact on the subject matter at hand.

(10) E8- Supreme court decides no expectation of privacy in regard to BFR

T4- Video surveillance moving from reactive to proactive

The results of this cross-impact analysis suggest that event 8 could have a positive 4 impact on trend 4. If the Supreme Court decides that there is no expectation of privacy in regard to biometric facial recognition, it would enhance the opportunity of video surveillance moving from reactive to proactive. In essence, it is felt that more time, money, and energy could be put into this research if there were no looming constitutional issues that may challenge the technology.

### Scenarios

Scenarios were developed based on input from the Nominal Group Technique and are often used to describe alternative futures. They are future stories that provide realism based on environmental scanning and the trends and events identified through the NGT process. Once a certain scenario is identified, strategic planning can be undertaken to plan for and influence the projected state or desired outcome. The three scenarios that will be presented below will describe pessimistic, optimistic, and normative futures.

#### Pessimistic View

Dressed in black slacks, a button-down, freshly starched pinstripe shirt, and a blue blazer, he would have fit in anywhere, especially in the crowded downtown financial district of San Francisco. It was 5:15 p.m. on Friday, June 13, 2008. After a busy week of deals made and

deals broken, it was party time for most of these highflying MBAs in the city renowned for its winter-like summers. Yet, this man was looking for a different type of party. Abdullah al Muhajire was a Yemen-born citizen, who, as of three years ago, had become one of al-Qaeda's top assassins.

Today would be the day that Muhajire had hoped to make national news. His family in Yemen only knew that he would not be returning from this trip to the United States. They had been taken care of financially, but that was of little concern to Muhajire's two small children, who had no understanding of the cause that ruled their dad's life. His wife of ten years had resolved herself to the fact that this was Allah's will and nothing she could do or say would be able to change that. She had said her goodbyes to Abdullah like she was saying goodbye to an old friend who had overstayed his visit. It was clear that Abdullah had changed over the years and that this cause had become the most important thing in his life, the family becoming a distant second.

John McKay was a stockbroker, who had just suffered through another bad week. Not particularly superstitious by nature, he began to wonder if the fact that it was Friday 13<sup>th</sup> had anything to do with a horrible day at work. The Dow had plunged another 750 points, and John had no idea where the bottom was. He had just endured another day of clients cursing him as the most inept stockbroker in the market. Daily death threats and intimations of lawsuits were coming from the same clients who used to send him \$500 bottles of wine for the millions he had made them.

John thought how funny life was. He had been on top just twelve short months ago, making millions and seemingly having millions of friends, but he soon found out that making millions and having friends went hand in hand. He was alone now and on the verge of losing his

job. This thirty-five-year-old Stanford MBA graduate never thought that the good days would end so quickly. What the hell, it was Friday the 13<sup>th</sup> and time to party. A few drinks and a few laughs with all the other soon-to-be-unemployed brokers would lift his spirits.

As John walked up California towards Sacramento Street to reach his favorite watering hole, he felt secure. The downtown area of San Francisco was equipped with state of the art video surveillance cameras that would be able to pick any face out of the crowd. It had been big news months ago, but they were hardly noticeable now. This was cutting edge technology that was now an exploding industry as security concerns became the number one issue for Americans. As John got closer to the Ireland 12 Bar, where he was sure a cold one would be waiting for him on the counter, he wondered how he had missed that biometric investment opportunity.

The system was so advanced that every terrorist, every wanted criminal, and all those on the watch list had been entered into a database that was capable of screening three hundred thousand faces very two seconds. If someone in the database was in the camera view, an alarm at the screening center would sound, and an officer would immediately be dispatched to arrest the suspect as the camera followed his or her every move.

John's losing streak was just about to get worse. Muhajire should have been immediately recognized almost a mile from the bar. He was in the database, as the CIA had information that he was a threat to attempt some non-specific terrorist acts in the Bay Area. But there must have been some glitch in the system. Muhajire unwittingly walked right through one camera zone after another. He was within one block of the bar before Muhajire finally tripped a camera.

The alert sounded as the screener immediately recognized the tragedy that was about to happen. He frantically called to his supervisor as Muhajire walked with a confident walk,

briefcase in hand, toward the pre-determined kill zone that would be packed with some of San Francisco's most elite. As the screener scrambled to alert the police, he quietly wondered how Muhajire had penetrated the protected zone.

John and Muhajire had reached the front door at the same time. Muhajire held it open for John, thinking, "Good, one more American pig victim," as John entered his favorite watering hole. The last thing that John heard was the unintelligible yelling from the polite Arab man who had just held open the door for him. John and eighty-seven other souls never knew what hit them as the blast from the briefcase leveled the building. This would be the first terrorist suicide/homicide bombing in the United States.

The headlines the next day read, "Biometric facial recognition system fails as eighty-eight die in preventable bombing." This would be the beginning of the end of the biometric facial recognition system. Politicians and citizens lost so much faith in the system that future plans for expansion were scrapped and never talked about again.

John would have been the first to sell short on this event, and he would have made millions. He would have used this to his advantage and would once again have been on top. He was the guy who could turn dust into gold, but his luck just ran out.

### Optimistic View

It was September 11, 2007, and the system was in place. It had been a long time in coming, but all knew that it would be well worth it. Facial recognition technology had come a long way very quickly in just six short years. The driving force was obvious as national security was the number one concern of the majority of Americans, thus it became the number one concern of most politicians.

The idea was simple. The technology had been developed so that it could recognize the face of any individual based on the space between their eyes, nose, and mouth. Experts called this the facial print, which is as accurate as a fingerprint. Every person has a unique set of bone structures and facial spacing.

The system was so advanced that it could detect cosmetic surgery and restructure the face like a map. The system could also see through clothing or disguises. High-speed cameras had been placed all around the city. They were nearly invisible thanks to advances in nanotechnology, which certainly pleased the environmental groups.

A sense of security enveloped the city, as it was evident that more and more citizens were venturing outside after the all-too-recent terrorist suicide bombings. This was the technology that everyone was waiting for to act as a blanket of security for the terrorist jitters that were now prominent.

De Costa was bent on evil. He was going to Washington D.C. to cause havoc. He knew that he would die in this mission, but this was his calling. He was not scared or glad to die, rather he had fallen into a state of numbness as he had reconciled himself to his fate.

De Costa didn't know cameras were in place. He had no idea he would be in a database that was meant as a net to capture him before he struck. As he entered the Washington, D.C., International Airport from the long plane ride, he was confident he would be welcomed into the country, as he had been dozens of times before. De Costa didn't know that things had changed. As he exited the plane, the alarms in the control room sounded. It was him the screener said. The computer had calculated the odds at 99.9999% positive on the identification.

De Costa, born in Brazil, started out as a drug trafficker. Soon thereafter he hooked up with al-Qaeda and received training in Afghanistan. He was a leader in al-Qaeda and only became a warrior when he was diagnosed with terminal brain cancer five months ago. He was going to die, so he might as well further his cause in death was his thought today.

His papers were in order. He was entering the country for cancer treatment at Johns Hopkins Hospital, known for its outstanding cancer treatment center. He would slide right through customs and be done with his deed and his life today. Everything he needed would be picked up at a safe house, for which he carried directions.

He never saw them coming. They looked like any other passengers in a busy airport, but the CIA was trained to blend in. The timing was perfect. A side door in the terminal flew open, and two guys suddenly had him by the arms. He was whisked behind the doors and away from public view. The system was working so well that this had been their tenth capture this month. Sure, the majority of the criminals were wanted for domestic crimes such as rape, robbery, and murder, but this was no tuna; it was a marlin. This would make front-page news.

The CIA had a way of getting information out of terrorists. Their means, though confidential, had been approved by Congress as part of the homeland security initiatives. Though dirty, it was effective. Operatives had the entire plan in less than two hours. In almost record time, three house raids would be conducted and sixteen more al-Qaeda members, along with bombs, guns, and more plans, would be confiscated.

The system was working. The facial recognition surveillance system has been the most effective weapon against crime to date. It has saved countless lives and has frustrated terrorist and domestic criminals to no end.

## Normative View

On this cold December 13, 2005, evening, the biometric facial recognition systems in place have worked, if nothing else, as a visual deterrent in a neighborhood once infested with drug dealers. The cameras are visible and cover a foursquare-block area previously referred to as the killing zone, appropriately named because if the drugs didn't kill you, the nightly turf wars would.

The technology is promising, but not there yet. Biometric facial systems of the future will be able to pick out wanted criminals as the system scans faces in a crowd. The accuracy rate is only at 65% right now, which has civil libertarians up in arms.

The protest continues as citizens try to balance personal security and safety against their right to privacy. The other area that is problematic is the aesthetic appearance of neighborhoods with these cameras. Budget concerns have been settled for now, as less officers are needed to patrol neighborhoods due to the impact of the cameras. This has created an issue with the Police Officers Association, who want to know if the camera is going to help them chase and fight with a drug dealer they have to arrest.

You can't argue with statistics, and crime is down in the killing zone. Only one full-time around-the-clock screener, who is more cost-effective than an officer, is needed to watch foursquare blocks that twelve officers previously couldn't control.

A lot will depend on the pending court decision regarding the holistic approach to policing with neighborhood cameras. That decision, which will be appealed by either side, is sure to drag on for years. In the meantime, one good capture through facial recognition or one false capture could decide the future of this technology.

## Summary

In chapter 2, the Nominal Group Technique identified specific trends and events that were likely to have a significant impact on how biometric facial recognition technology will impact the prevention of crime and terrorism. The three scenarios present very possible alternatives to the issue statement. The NGT and accompanying scenarios will help in developing a strategy for change that will be outlined in the following chapters.

## CHAPTER THREE

### STRATEGIC PLAN

The police organization, which will be developing a strategic plan, is the Blue Pacific Police Department. The city of Blue Pacific has a diverse ethnic population consisting of 950,000 residents. Located in the Bay Area, it has 50 square miles of hilly streets and breathtaking views. A very strong mayor and a diverse board of supervisors, who are elected according to the eight different districts where they reside, govern the city. The Blue Pacific Police Department has 1700 sworn officers and is often the center of controversy, in large part due to the liberal beliefs of the majority of the voters. The American Civil Liberties Union plays a major role in city politics.

Often the center of demonstrations, due to the mayor's encouragement of free speech, Blue Pacific is also a world-class city that attracts millions of visitors each year. The downtown area is vibrant and well-known. The city in general, like many other metropolitan cities, is a cultural melting pot encompassing a range of dwellings from exclusive neighborhoods with million dollar homes to tenement slums.

Though the city of Blue Pacific has a proactive approach to policing, it has one of the highest violent crime rates in the country for a city its size. The FBI has advised Blue Pacific that because of its tourist attraction, it has been identified as a viable and probable target for terrorism.

A strategic plan will be developed for the Blue Pacific Police Department, which will utilize a structured approach to comprehensively explore issues of concern as they relate to the utilization of biometric facial recognition systems within the city. The desired outcome of a strategic plan is to help facilitate and manage a specific goal for the Blue Pacific Police

Department. It is important to remember that key issues of today may not be of relevance in the future; therefore, an organization must balance current and future needs. The Blue Pacific Police Department organizational leaders charged with the implementation of this plan must constantly seek opportunities to bring about positive change. Strategic planning allows organizations to capitalize upon positive trends and events identified in the Nominal Group Technique while allowing an organization to avoid trends and events that will have a negative effect upon the desired goal.

A strategic plan for the Blue Pacific Police department will be developed to assist with the implementation of biometric facial recognition systems throughout the city in an effort to prevent crime and terrorism. Information from environmental scanning, as well as the Nominal Group Technique, will be utilized in this process.

### Vision Statement

In order to keep all involved parties focused on the desired outcome, it is imperative that a vision statement be developed. The vision statement must represent the core values and overall objectives of the organization and set a course of travel for what the organization wants to achieve and how it will get there. The following is a vision statement for the Blue Pacific Police Department that will be utilized to achieve their stated goal:

“It is recognized that Blue Pacific’s Police Department’s primary responsibility is to provide the highest degree of public safety possible, while protecting the privacy interest and rights of all citizens as guaranteed by this country’s Constitution. It is also recognized that we are living in troubled times wherein conventional means of protecting the public have become antiquated or ineffective. It is further recognized that we are also living in a technological age wherein advanced computer technology has been developed to a point where it can act as a viable tool to assist law enforcement with the huge responsibility of protecting the public. Biometric facial recognition technology is a controversial, yet proven effective tool in the identification of wanted individuals. With the

ultimate protection of our citizens in mind, members of the Blue Pacific Police Department are committed to assisting with the development, implementation, and deployment of biometric facial recognition technology in public places. The Blue Pacific Police Department will institute a program that sets clear guidelines on how this technology will be used to assist us in the apprehension of wanted individuals and terrorists, while ensuring that the privacy interest of the public is maintained.”

### External Analysis - The STEEP Model

External pressures can induce significant change in an organization. One method of analyzing these external pressures is through the Social, Technological, Economic, Environmental, and Political (STEEP) model. Through the use of these five areas, the STEEP model can scan for external signals that may have an effect Blue Pacific Police Department’s desired change. The results of the STEEP model may have a profound impact on how Blue Pacific P.D develops its strategic plan, or if biometric facial recognition technology should be implemented in an effort to prevent crime and acts of terrorism. The next section will look at each of the five specific perspectives and examine some of the issues that should be addressed when implementing a biometric facial recognition program.

#### Social

Privacy rights have a significant influence on the implementation of any biometric facial recognition system. The City of Blue Pacific is an extremely diverse and, at times, liberal city that places a high value on individual rights and the right to gather without government interference. The thought of big brother watching over citizens of Blue Pacific will be extremely distasteful to those who put a high premium on privacy, even in the wake of increased threats of terror. Many will also be concerned about Blue Pacific Police Department’s future ability to link

databases that already exist, which will ultimately allow police to track the movements of individuals. There is a perceived potential for this technology to stifle peaceful demonstrations and public gatherings for fear that individuals would be captured on film and labeled by government entities.

Civil libertarians will also claim that there is the real possibility of this technology being abused to racially profile minority groups.<sup>53</sup> Citizens will clearly be concerned about information that is collected and maintained about them. This must be balanced against the social need to feel secure and safe. Prior to September 11, 2001, citizens of this country had never been in such fear of attacks in their homeland. Since then, most citizens seem to be willing to give up some personal freedom in order to secure their safety. This may have a profound and long-lasting impact on the way and with whom they socialize. There is also fear of false detentions and arrests based on faulty and inaccurate technology. From a social perspective, a balance must be maintained between perceived violations of privacy and the need to protect the public.

Additionally, there is an ever-increasing transient population in this country that puts law enforcement at a distinct disadvantage. People are more mobile, and it is becoming increasingly difficult to track and capture wanted individuals. But, the reality is that in order to get around, one must often use transportation systems. These areas may be the best location and the least intrusive to first implement this technology.

### Technological Issues

The San Francisco Bay Area currently is one of the best spots in the country for the development of technology. After the recent technological downturn, the Silicon Valley is

poised for a rebound and has much of the technological brainpower and equipment in place to work on security-related technology. Currently, there is no regulation of biometric facial recognition technology in public places, but this area, like wiretaps and other government security measures, will be ripe for regulation. Blue Pacific Police must closely monitor any regulations in the biometric recognition area, which could have a chilling effect on the industry as a whole.

Technology is expanding and improving at an exponential rate. It is imperative that Blue Pacific Police implement this technology in a thoughtful way for the right reasons, otherwise, there is great potential for it to grow too much, too fast. This could ultimately lead to the demise of the technology if an ill-informed society revolts against it. It will be important for this technology to be viewed as a security tool rather than a surveillance technique because of the negative connotation that the latter has.

Certainly, an advantage to this technology is that it is one of the least intrusive of the biometric family. You don't have to give blood, place your finger somewhere, or step up to machine and have your iris scanned. As this technology grows, the public in Blue Pacific will simply be able to walk about as they normally do while a computer processes their image.

### Environmental Impacts

In the United Kingdom, there are currently over 2 million security cameras in operation.<sup>54</sup> From an aesthetics standpoint, some feel that cameras in public places are detractors from natural beauty. This may be especially true in a City as beautiful and world renowned as Blue Pacific. There is a feeling of being unable to enjoy the surrounding environment because of the constant feeling of being watched. The NIMBY (Not In My Backyard) theory is alive and well when it

comes to security cameras. People want to feel secure, but they don't want to feel like they are being watched.

There is an additional question about the effectiveness of biometric facial recognition systems. Do they really act to prevent crime and terrorism, or do they simply act to displace the crime to surrounding neighborhoods that are not being watched? It is really too early to tell, but this will have to be closely monitored.

### Economic Considerations

There may be no time better than now to be involved in biometric technology. Globally, in 2002, the biometric industry revenues were at 601 million dollars. By the year 2007, the biometric industry is expected to top 4.04 billion dollars, driven by the large-scale deployment of biometric security products.<sup>55</sup> Biometric facial recognition currently holds 11.4% of the whole biometric field, which is second only to finger-scan.<sup>56</sup> In this time of economic downturn in technology, this industry could give a huge boost to the unemployment rate. Additionally, there is substantial private money sitting outside the market looking for viable technology in which to invest. The biometric industry could very well be the next dot-com industry that takes the United States out of its current economic slump. If the City of Blue Pacific implemented biometric facial recognition technology in public places, they would be on the cutting edge of an emerging technology that may take root in the San Francisco Bay Area.

The other promising aspect about biometric facial recognition systems is that it has a potential to save personnel costs. Companies could hire less security or fewer police because of the potential widespread application of facial recognition systems. Large geographic areas that exist in Blue Pacific like buildings or downtown areas could be monitored by remote command

centers at the Blue Pacific Police Department, which could then dispatch police if a wanted individual or terrorist was located.

This technology could also have a profound impact on Americans' travel habits and tourism in the United States. The City of Blue Pacific is a major travel destination that has been severely impacted by the threat of terrorism. If people felt they were in a safe environment, this could lead to more travel and an increase in tourism.

### Political Impacts

Historically, law enforcement has been expected to do more with less, complicating the politics of money allocation. Politicians are very leery about spending money on emerging technology, especially when it is controversial and will be perceived by some as impinging on their privacy rights. The City of Blue Pacific is no exception and the mayor and county supervisors are constantly looking for ways to save money, especially in election years. The political reality is that sometimes-elected officials are forced to do what is popular, which is sometimes incongruent with doing what is right. There could be tremendous resistance to the implementation of this technology in the Bay Area because of its pro-privacy climate.

There will be a difficult distinction to be drawn between providing more security to the citizens while ensuring that privacy rights are not trampled. This need may lead to legislation that may limit the time and place of when facial recognition technology may be used, and it might lead to notification of the public prior to its use.

## Analysis of the Organizational Culture

Planning for change is a key component to any organization's continued health. All organizations, public and private, must constantly and objectively check the internal temperature to ensure that they are healthy and not stuck in the status quo, but moving in a coordinated and comprehensive manner toward the future. It is very important for leaders of an organization to understand if members of an organization will resist or support change. One model that can be utilized to help with the analysis of change is the "WOTS UP" (weaknesses, opportunities, threats, and strengths underlying planning) model. Using this model the following is an analysis of change that could impact the Blue Pacific Police Department internally.

### Weaknesses

Though currently evolving, Blue Pacific Police Department lacks the technical knowledge to rapidly implement technological advances. In fact, though most security technology originates with the military, law enforcement is usually one of the last entities to implement it. Technological advances are sometimes looked upon by Blue Pacific police officers suspiciously as a means of possibly taking jobs. Facial recognition may be looked upon as a way to monitor large geographic areas or transportation hubs within the city of Blue Pacific with the use of technology rather than police officers.

The other area of concern for Blue Pacific Police Department is the expense and training time that biometric facial recognition technology will require. The Blue Pacific police officers are constantly being asked to accept some new form of technology and may be at the saturation point. Another area of weakness is the concern about reliability and consistency. Current technology does not adjust well to different lighting conditions, disguises, and backgrounds.

There is a fear that wanted individuals or terrorists could slip by the system, which law enforcement in the city of Blue Pacific may come to rely upon too heavily.

### Opportunities

The Bay Area is one of the best technological centers in the world, yet it has been decimated by the dot-com bust. On the contrary, there are considerable amounts of private money available for investment in viable products. The city of Blue Pacific could capitalize on the combination of brilliant technological minds and availability of money. With the threat of increasing crime and terrorism, and Blue Pacific officers' desire to keep the public safe, an opportunity has presented itself that makes the timing of this technology appropriate for exploration.

Due to budget constraints, Blue Pacific P.D understands the need to integrate services and share information. Crime is not faceless and there is an incredible facial database that is ready to be tapped into to identify suspects. Blue Pacific officers may have the ability to readily identify suspects before they strike again or use the technology to prevent a terrorist attack. Potentially, Blue Pacific police have the ability to save thousands of hours searching for suspects by allowing a computer to search through six million photos a minute for a facial match. Blue Pacific Police Department takes great pride in its ability to capture suspects and bring them to justice to pay for crimes committed. Biometric facial recognition may allow Blue Pacific officers an opportunity to provide better service to the public it has sworn to protect.

## Threats

One of the greatest threats to facial recognition is the overregulation of this industry, which will act to frustrate Blue Pacific Police Department's purpose and goal of preventing crime and terrorism. If Blue Pacific police are forced to seek search warrants before using this technology or warn citizens of its use, it could be viewed by agencies as a tool that is more trouble than it is worth.

Another drawback could be improper use of this technology. Misuse could cast a law enforcement agency as a racial profiler, which could lead to sanctions.

Officer safety is a huge aspect of police work, and any attempt to replace staff with machines may bring protest from the Blue Pacific Police Officers' Association. There is also the continued threat that the city manager or local government officials may not go along with the program. Or, the costs of the program may outweigh the benefits. Placement of cameras in public areas may simply relocate crime instead of preventing it, bringing more calls of complaints to police.

## Strengths

The incredible power that could potentially be harnessed by law enforcement with biometric facial recognition is the strength of this program. The possibility of suspects having no place to hide from law enforcement is exciting. Law enforcement agencies would have the ability to talk with each other and throw out a net so wide that it would not matter if a suspect fled to another state, because somewhere a camera would capture the suspect's face and he or she would be caught. The potential resource-saving possibility is a huge strength of this program. The potential for private/public ventures in the name of public safety is an exciting

prospect. The potential to provide citizens with peace of mind and a feeling of safety is a real possibility with this program.

### Other Considerations

In order for any plan to be successful, the Blue Pacific Police Department must first identify all the stakeholders and identify what part in the plan they are likely to play. Stakeholders are individuals who will somehow have a vested interest in Blue Pacific's Police plan and can impact it in a positive or negative manner. Overlooking a stakeholder, no matter how small, can have a dire impact on one's ability to implement a plan. Stakeholders can be internal or external to the organization, yet they all share the same trait of being able to influence the plan in varying degrees. It is essential to identify all stakeholders so that they can work in a collaborative effort to help bring the plan to fruition.

The person charged with implementing the plan must understand the role that the stakeholders play. Stakeholders may support the plan, oppose the plan, or be somewhere in the middle. The person charged with implementation of the plan must maintain the confidence of the supporters and those on the fence, while generating the support of the individuals opposing the plan. An alternative would be to incorporate the opposing views into the implementation plan. The stakeholders involved in the implementation of a biometric facial recognition system along with their roles are as follows:

- Blue Pacific mayor and board of supervisors

These are the plan reviewers and developers. They are responsible for financial support. They are critical for the long-term sustained support of the plan. They also have been strong supporters of the Blue Pacific Police Department and will have to balance their usual support for

safety programs against the public's right to privacy. They are the policy makers who are committed to providing Blue Pacific Police with the tools they need to do their jobs. They usually like to support their police Department and, in turn, may look for support from their police. They tend to fight a lot with each other, but tend to agree on public safety issues.

- Blue Pacific city manager

The Blue Pacific city manager will review the plan and be involved in implementation. She will control the financing and will determine if the plan is brought to the city council for approval. The Blue Pacific city manager is responsible for the overall staffing of the city. She answers to the city council and she is committed to providing the highest degree of public safety. Though the city manager has been very supportive of the Blue Pacific Police Department and its public safety initiatives, she must also consider the benefit in relation to the expense. The Blue Pacific city manager has a keen understanding of the political climate of the city and fully understands the feelings of the voters. It is believed that based on the city manager's usual track record of supporting crime-fighting efforts, she will want to support the police department's implementation of biometric facial recognition systems.

- Blue Pacific police chief and management

These are the program managers, developers, and implementers. They will also direct and oversee the policies. They will be responsible for operations of the police department and the hiring and training of employees. The Blue Pacific police chief and management staff plan services and implement policies for policing of the city. They have responsibility for the allocation of resources and for the implementation of technological advances. The chief and management will be very supportive of the biometric facial recognition technology due to its low cost in relation to staff members along with the possibility of reducing crime.

- Blue Pacific police labor union

This is a politically-positioned employee group interested in officer safety issues and the safety of citizens. They will look to save police jobs but are open to innovative technology that will give them another tool to catch criminals or prevent crime.

- Blue Pacific community

The Blue Pacific community is concerned with public safety and the fiscal soundness of government decisions. Likewise, they are concerned with their right to privacy and can be averse to too much governmental intrusion. They are a powerful group that will dictate how the city council responds to an issue. For the most part, the community of Blue Pacific is very supportive of police initiatives and is very pro law and order. The community favors giving more tools to the Blue Pacific Police Department, which may result in a safer society.

- Blue Pacific finance director

The Blue Pacific finance director is responsible for the fiscal soundness of the city. He is very restrictive with the city's money and is usually not open to innovative or untested technology. He will take part in the decision to determine if there are appropriate funds to implement the plan and it will be very difficult to sell him on this idea.

- Blue Pacific city attorney

The Blue Pacific city attorney is responsible for overseeing the legal consequences of decisions made by the city. He will have to defend any lawsuits brought on behalf of citizens, and he acts as an advisor to the city council. The city attorney will also be a likely partner in drafting the policies regarding the use of facial recognition systems in public areas. He is very pro law enforcement and will look for legal ways to achieve the police department's goal.

- Blue Pacific department head board of directors

They are charged with the overall city direction on programs and expenditures. They are responsible for reviewing the pros and cons and then making an informed decision on the direction the plan should go. They will examine the fiscal soundness of the program and weigh the program using a cost benefit analysis. They will be a very difficult group to present this issue to, due to their conservative views and frugal spending habits.

- Blue Pacific private enterprise

They are the providers of biometric facial recognition technology. They are located within the city of Blue Pacific and look for the Blue Pacific Police to be partners with them, as the technology is developed to meet their needs. There will be opportunities to be a beta test site for this evolving technology at little cost to the organization.

### Snail Darters

Snail darters make up the unforeseen or unanticipated group that can impact a strategic plan at a critical moment. It is imperative that they are identified and Blue Pacific Police Department be prepared to respond to their particular issues.

- Blue Pacific Civil Libertarians

Civil libertarians are firmly entrenched in the city of Blue Pacific. They have a strong interest in keeping the city free from government intrusion. They will take up a cause wherever it is and will stage protests or attempts to influence public opinion. At times, they have a very strong voice and will support the Blue Pacific Police Department on public safety issues, as long as the issues do not impinge on privacy rights. They have taken a non-supportive stance on the subject of biometric facial recognition technology.

- Legislatures

They are responsible for passing laws and dispensing of funds. This group will either keep their hands off this issue or pass restrictive legislation on its use. They could also assist local police agencies by funding this project.

- Press

The press is responsible for reporting news in an unbiased manner. The problem is they have the power to put a slant on news to meet their own interest. The press is a very powerful stakeholder that should never be forgotten.

### Development of Alternative Strategies

When implementing a strategic plan, it is necessary for the Blue Pacific Police Department to consider alternatives. Three alternative strategies have been developed for the Blue Pacific Police Department to show how the implementation of biometric facial recognition could impact the prevention of crime and terrorism:

Strategy 1: Maintain the Status Quo

With the rising question of the accuracy of biometric facial recognition and the concerns surrounding privacy issues, the promising future of biometric facial recognition may not ever reach Blue Pacific Police Department's desired goal. Since September 11, 2001, there has not been a large-scale terrorist attack inside the United States, and it appears the American people are starting to put fear of terrorism behind them. This is evidenced by an increase in travel and more protest about civil restrictions.

Crime rates in the City of Blue Pacific will go up and down with the economy and biometric facial recognition may be a false blanket of security to a city looking for a cure to fix the social problems of this country.

This technology may be too costly and provide too little help in relation to the resources that it would take to run it. The cost to Blue Pacific citizens' privacy rights may be too great for the return that the Blue Pacific Police would get from this technology. Taking no action to explore or implement this technology would be the simplest strategy of all, but it does nothing to prepare the Blue Pacific Police Department for the year 2008 and future terrorist attacks. By the time the Blue Pacific Police Department acts after another attack, it will be too late. A failure to act today will be at the expense of the citizens of Blue Pacific tomorrow.

#### Strategy 2: Restricted Implementation Plan

Biometric facial recognition technology can be implemented in the City of Blue Pacific today in a restricted structure that will allow officers to take suspect photos or sketches and place them in a database of images in search for matches. This will act to save officers countless hours of research and expand the net reach of Blue Pacific Police. This will be the least controversial as it is applied after the fact, in that the crime has already occurred, there is an image, and the police will try to match that image against a database. This will allow for the potential apprehension of suspects after the fact and before they can victimize again. This is a powerful tool in the prevention of additional crime and has proven to be successful in the past. Bank video surveillance film can be encoded into the system and the system will be searched for the suspect. If it is a good photo and the suspect is in the database, there is likelihood that the Blue Pacific Police will identify and apprehend the suspect.

Though this is a great reactive tool, it does nothing to prevent terrorism or victimization before the crime occurs. It will not allow police to observe wanted individuals and take them into custody on the spot before they can strike citizens of Blue Pacific. Though this plan is a large step in the right direction, and could be part of a strategic implementation plan, it will not allow the Blue Pacific Police to harness the full capability of biometric facial recognition technology.

### Strategy 3: Full Implementation with Guidelines

Public safety is so important to the City of Blue Pacific that the police would be remiss if they didn't use all the tools at their disposal to take criminals off the streets before they strike. Why should citizens of Blue Pacific wait until a child molester strikes at a playground? Why does Blue Pacific Police let thousands of wanted individuals walk around the streets with immunity? The answer is that the Blue Pacific Police Department does not have the resources to be all things to all people. Yet there is technology available that will assist them to identify suspects and track them even if they don't have the resources to physically be there.

The Blue Pacific Police Department could create a local database of wanted individuals. Cameras could be deployed in strategic locations around the city and its airport to capture and cross-check images against wanted individuals in the database. In conjunction, crime-free zones could be created and monitored for criminals.

The Blue Pacific Police Department must develop strict guidelines on how these systems can be used by its law enforcement officers. The police must ensure the public that the systems will not be used to create profiles on individuals or to create a national ID card system.

The real solution may be a combination of the three options with a phased-in approach. This will allow for a slow, open approach that will allow critics to gain knowledge about

biometric facial recognition systems. It will also allow the Blue Pacific Police Department the time to put procedures in place and train personnel. Ideally, this project should be phased in over a four-year period of time with plenty of public outreach efforts on the part of Blue Pacific Police Department.

### Summary

Chapter three examined a structured approach to prepare the Blue Pacific Police Department for bringing about its desired change in policing to develop a higher degree of safety for its citizens. An internal and external analysis of the organization was examined, stakeholders were identified, and alternative solutions were explored. Three different options for the city of Blue Pacific have been explored. The best option is a phased implementation plan involving all three options over the next four years.

With the groundwork set for the proposed program change within the police department, it is very important that a comprehensive plan be developed to implement the change. Chapter four, Transition Management, addresses this plan.

## CHAPTER FOUR

### TRANSITION MANAGEMENT

#### Introduction

Transition planning is a crucial step in the overall success of a new program, particularly one that might be implemented in stages and will encumber resources or finances. There are many ways for leaders to make the transition to the future, but it is imperative that it be done in a well-thought-out manner with support of stakeholders and identification of all the issues that could ultimately impact the change.

The development of a biometric facial recognition system that can detect wanted individuals or terrorist in the City of Blue Pacific must be extensively researched and extremely well managed. The decision-making nucleus of the Blue Pacific Police Department will ultimately be held responsible for the successful transition of change. This project will use John P. Kotter's manual entitled, "Eight-Stage Process of Creating Major Change."<sup>57</sup> The transition planning uses some of the same measures utilized during the strategic planning process and can assist in directing the Blue Pacific police organization in change. The eight stages are as follows:

#### Establish a Sense of Urgency

As used previously, scanning the environment is one method used to identify external forces that can impact change in a law enforcement agency. Monitoring court cases, keeping a finger on the pulse of public opinion, and staying informed on the latest innovations regarding this technology would put the Blue Pacific Police in a better position to create change. For this particular issue, citizens must understand that facial recognition has the potential ability to take

dangerous criminals off the streets of Blue Pacific before they strike. This has the potential to save valuable police resources making an officer's job easier.

Crimes are not faceless so let police work with the citizens of Blue Pacific to catch criminals. The City of Blue Pacific has the ability to create a feeling that criminals will have nowhere to hide so they should just turn themselves in. If the city waits for crime to occur, it could be too late for many innocent citizens. Creating sense of urgency will act to establish the importance of this topic while generating buy-in from internal and external sources.

It will be essential for the Blue Pacific chief to put community police officers in charge of this assignment. Community police officers have the trust of the citizens and are extremely well-known in community groups. They have the public communication network available and will be able to create a critical mass of citizens to support this project. This will give the Blue Pacific Police Department the ability to place a controlled message out to the public in small groups where questions can be answered in a civil setting.

In addition to marketing this sense of urgency to the public, the Blue Pacific Police Department must also target the city manager, mayor, board of supervisors, and the press. These are the people that will help create the critical mass that will be needed to implement biometric facial recognition systems in public places in the City of Blue Pacific.

### Create the Guiding Coalition

The selection of key personnel with power in their position, broad expertise, and high credibility is important to change. This would include personnel within the Blue Pacific Police Department who work violent crimes, who work with technology and crime analysis, and who demonstrate the contagious enthusiasm to lead an organization through change. This must be a

person or group who is willing to talk with others, inside and outside the police department, and appeal to their sense of being part of a noble cause. This is the person or group that the Blue Pacific Police Department will have to trust implicitly to lead the organization to change.

A police captain with broad expertise in technology, public relations, and who is respected by both the public and city staff should be assigned to this role. It will be important to get a critical mass of officers to buy into this project in the early stages. The captain should meet with small internal groups and explain the plan. It will be very important to get the Police Officers Association to buy into this as a first step. The Captain should create a group consisting of a cross section of the police department and that cross section should be in charge of the marketing plan and implementation plan.

Again, this group must understand that the marketing needs to target not only the public, but also the city manager, department heads, mayor, board of supervisors, press, and snail darters. This group will be charged with developing a comprehensive, multifaceted rollout plan to address the inevitable concerns of its target audience.

### Developing a Vision and Strategy

The chief of the Blue Pacific Police Department, as leader of the organization, has to set a vision of what the organization hopes to achieve. The goal must be realistic and attainable. It may be simply to implement biometric facial recognition technology to help police identify wanted individuals, or it can include the deployment of facial recognition in public places. The leader must be aware of limitations and must not go too far too fast. The leader must also be flexible and be ready to change directions if the direction they are going is not working. The

Chief of the Blue Pacific Police Department must establishing short-term goals as a good way of ensuring that the overall goal is met.

It must be very clear that the chief supports this project and what the benefits of this project are. The message to the staff should come directly from the chief who must underscore the urgency for the successful completion and implementation of this program.

The Blue Pacific Police Chief must be ready to address the city manager, board of supervisors, press, and critics of biometric facial recognition systems and have a very good explanation how this will help provide for a higher degree of public safety in the City of Blue Pacific.

#### Communicating the Change Vision

Accepting a new vision can be a traumatic ordeal for those impacted members of the Blue Pacific Police Department as well as the public. It is essential that the vision be shared with all members of the department and public and that there be time for clarification. If the vision is not fully understood, it cannot be fully shared. This is one of the most crucial points in transition planning. Repetition, they say, is the key to learning; well, it is also the key to buy-in. Once the vision is communicated, leaders must act in a manner consistent with their message. In this case, actual steps toward the implementation of facial recognition should be taken to promote buy-in and establish credibility.

The creation of small study groups consisting of a cross section of the police department and public should be established independently. These groups should be used to test and refine the message that will be sent to the organization and public. Once the program is underway in

the City of Blue Pacific, it will be essential to updates staff and the public on the progress of the program.

### Empowering Broad-Based Action

Personnel must be empowered to remove as many barriers that stand in the way of the vision as possible. The vision must be communicated to employees and then structures must be made compatible with the vision. Employees of the Blue Pacific Police Department must be given proper training and should work with outside organizations to deal with non-traditional approaches to identified problems. An example would be police and private industry working together to create a system that uses biometric facial recognition in public places without resulting in the storage of non-criminal faces in a national database.

The group that was identified in the guiding coalition section should work together to develop an understanding of what their needs are and what they hope to achieve with biometric facial recognition technology. They should then relay those needs to outside industry to ensure that the needs of the organization are meet.

### Generating Short-Term Wins

Short-term wins are visible, are unambiguous, and clearly can be connected to the desired change. These wins encourage and energize everyone associated with the change. A great short-term win could be to identify one suspect through facial recognition technology in the first year of implementation. It will be important for the department's press information officer to exploit this short-term success to the benefit of the Blue Pacific Police Department. This will also allow the guiding coalition to have some feedback on the soundness of their vision. It provides for an

opportunity to change the vision if necessary and really acts as a check and balance. Short-term wins also allow the Blue Pacific Police Department an opportunity to convert non-believers into believers.

### Consolidating Gains and Producing More Change

Short-term wins can be turned into long-term gains. Short-term wins are a mechanism used to tackle bigger projects involving change. This type of change could be the creation of a facial recognition unit within the Blue Pacific Police Department that is dedicated to using the technology to find wanted individuals. It creates a bigger backing by bringing more people into the project, which acts to create more excitement about the possibilities of the project. It may expand into a countywide task force or statewide task force. This opportunity within the Blue Pacific Police Department should not be overlooked.

### Anchoring New Approaches in the Culture

As change takes place in law enforcement, it is important to bring a culture of change to the Blue Pacific Police Department. This is imperative in the promoting, hiring, and training process and change must be understood as a norm rather than an exception. The organization as a whole must be looked at as one. The organization must be tolerant to change and actually embrace it.

### Additional Steps

Since this subject matter also involves national security, Blue Pacific Police Department must seek help from the United States Federal Government, which must take an active role in the

research and development of this technology by partnering with private industry. The Blue Pacific Police Department must work with law enforcement as a whole to create a national database of images that will allow for faces to be encoded and checked against the database for wanted or known dangerous individuals. Other large, urban law enforcement agencies must work to deploy this technology in all transportation hubs in an effort to stifle the movement of terrorists and wanted individuals about the country. This will allow for an easier transition period for the Blue Pacific Police Department in the deployment of this technology.

At the local level, large, urban police departments must start working on the implementation plan for this technology in the Bay Area. To that extent, the first steps must be development of criminal image databases, exploration of the latest technology, and identification of the stakeholders. In the Bay Area, possibly more than any other place in America, biometric facial recognition technology will be a very difficult sell. The Bay Area is well-known for its liberal views and suspicion of big brother. This stance calls for a comprehensive public education program that will bring about mutual cooperation of all the stakeholders in the name of security.

To ease the suspicion and engender a feeling of trust, state guidelines on the appropriate use of stored facial recognition data must be established. This program should also involve the immediate and comprehensive training process that law enforcement should undergo to understand how this technology works and how it can prevent crime and terrorism.

Failure to act at this time could create a technology gap that may be insurmountable in a future time of crisis. By acting now, law enforcement allows itself the time to create a strategic implementation plan for the deployment of this technology. This will allow law enforcement the opportunity to create a crime prevention tool in incremental steps. Federal homeland security

grants should be issued to law enforcement agencies hoping to participate in this program. Law enforcement agencies across the country should work together to ensure that the federal government sets aside funds for the protection of Americans through the development of biometric facial recognition technology.

### Summary

The implementation plan to establish biometric facial recognition systems in the Blue Pacific Police Department will be a crucial step in the process. It goes against the grain of traditional policing where officers look for bad guys. Biometric facial recognition can have a profound impact on personnel and the traditional ideology of policing. This chapter examined the crucial steps and key individuals necessary for the implementation process.

Chapter 5 will consist of a summary of this project, recommendations, and conclusions.

## CHAPTER FIVE

### SUMMARY, RECOMMENDATIONS, AND CONCLUSIONS

#### Summary

The need for law enforcement to fight crime with new biometric facial recognition tools has been addressed throughout this project and forecast to the year 2008. This was accomplished through exploration of the issue using environmental scanning, research review, interviews, and case studies. An NGT panel was used to examine trends and events that were thought to be associated with this issue.

This project presents the position that the use of biometric facial recognition by law enforcement will help to prevent crime and terrorism in the United States by the year 2008. This position is based on the fact that society is in a new age of heightened security. September 11, 2001, changed the landscape in the United States forever. Criminals and terrorists are becoming more mobile, and increased crime and terrorism is almost a certainty in the United States over the next several years. Fear for personal security has a profound chilling effect on the national economy. People are afraid to travel and the tourism business has plummeted as a result of security concerns.

Though the City of Blue Pacific, a large, urban law enforcement agency, was chosen for this model project, the basic premise of using biometric facial recognition technology to increase security and prevent crime and terrorism is applicable to all law enforcement agencies. Once the preferred option, namely, development, implementation, and deployment of biometric facial recognition technology in public places, was articulated in a vision statement, specific implementation strategies were presented to help the process of change. This project then

addressed steps for realizing the transition management plan to ensure overall success of achieving the desired result for the Blue Pacific Police Department.

### Recommendations

It is imperative that the Blue Pacific Police Department and other law enforcement agencies act now and in a united way. As explored earlier in this project, one of the major obstacles that law enforcement faces is the inability to communicate with each other. Law enforcement has no idea of who is wanted in neighboring jurisdictions; they spend precious resources trying to identify suspects who have committed a crime and have been caught on tape. Unless the suspect lives locally and a law enforcement officer happens to know him by sight, police stand very little chance of clearing that case. Suspects with a prior arrest commit the most violent crimes, and their facial image is already in a database. The government possesses thousands of photos of known or suspected terrorists. The technology that will allow law enforcement to readily identify these individuals is evolving with rapid speed, so that they can be taken off the street before they victimize again.

It is recommended that the Blue Pacific Police Department deploy biometric facial recognition systems in phases. The first phase would be the use of the system to scan the images of criminals caught on film against a known database to establish identity. This phase should take place immediately: It can be accomplished with very little resistance from the public and can be a great asset to officers who traditionally have to search thousands of pictures to establish a suspect match.

The next phase would be to establish internal and external groups, (including members of the snail darters), who would help establish how and where biometric facial recognition could be

utilized in public places. They would also help create the marketing plan for this change. The group could utilize this technology at the Blue Pacific airport where lighting can be controlled and where citizens are use to being scrutinized. The Blue Pacific Police Department should then continue to work with the public and private industry to develop a reliable biometric facial recognition system that is capable of being deployed in public places. This entire phased plan should take place over the next five years.

### Conclusion

If immediate steps are not taken to further develop national image databases and deploy biometric facial recognition systems throughout the United States, the future of local, state, and national security looks bleak. The Blue Pacific police continue to be frustrated by the thousands of wanted individuals who walk the streets every day and commit more crimes because no one knows that they are wanted. Clearly, terrorism is on the rise and on September 11, 2001, terrorists showed that they could strike at the heart of America.

Citizens need not wait for the next terrorist to walk through another United States airport undetected. The public need not wait for the next wanted suspect to be caught in the act before they are arrested. The Blue Pacific Police Department has the opportunity to make it very difficult for terrorists and criminals to live in and move around its city with immunity. If the Blue Pacific Police Department acts now, biometric facial recognition technology can make its city a much safer place by the year 2008. Imagine a place where wanted individuals turn themselves in because they have no place to hide. Imagine a secure city where terrorists refuse to come because they will be detected at the border or as they move about the country.

The problem of securing the City of Blue Pacific will not be solved overnight. Additionally, biometric facial recognition is not the stand-alone answer to all security concerns. Looking into the future, the prevention of crime and terrorism is not going to get any easier for the Blue Pacific police; therefore, law enforcement has to continue to strive to look for opportunities in technology to achieve this goal. Crime is not faceless, meaning every criminal and every terrorist has a unique face. Unlike any other technology, biometric facial recognition has the potential to cast a wide net across the nation in search of threats to society. This technology has the promise of being the least intrusive of the biometric family. Physically, it doesn't require the suspect to do anything but walk by a camera, something that almost every American does on a daily basis without even knowing it.

Developing a biometric facial recognition system to assist, rather than replace law enforcement, is not only needed, but it is also the right thing to do in securing the City of Blue Pacific from internal and external threats. The Blue Pacific Police Department leaders must bear in mind that their duty is to protect its citizens today and tomorrow.

## APPENDIX A

### NOMINAL GROUP TECHNIQUE PANEL MEMBERS

Dennis Caines, Assistant City Attorney  
City of San Mateo

Mr. George Grotz, Director of Sales  
Data911

Mr. Paul Lego, CEO  
Virage Corporation

Wende Protzman, Senior Management Analyst  
City of San Mateo

Robert Ross, Police Sergeant  
San Mateo Police Department

Alicia Santamaria, Management Analyst  
San Mateo Police Department

Ed Trucco, Retired Police Captain  
San Mateo Police Department

APPENDIX B  
LIST OF TRENDS

1. Homicide/suicide bombings
2. Paperless money crime/technology
3. Aviation security
4. Facial improvement technology
5. Increase homeland security legislation
6. Internet intelligence gathering – foreign and domestic
7. Level of public/privacy expectations
8. Level of personal privacy expectations
9. Increase video surveillance - proactive
10. Increase G.I.S. information
11. Increase awareness biometrics
12. Technology savvy
13. Reduction of funding – Biotechnology (decrease in local government funding; increase in national government funding)
14. Level of civil liberties due to terrorism
15. Level of cooperation between police and media
16. Amount of groups opposed to increased surveillance
17. Reliance on DNA and scientific evidence to convict or release subjects
18. Lack of unity in our country
19. Commitment to develop biometric standards

20. Level of cooperation by local, state, and federal agencies
21. Defense groups questioning validity of scientific evidence
22. Racial profiling
23. Technology vigilantism
24. Sophisticated criminals
25. Interoperability voice data
26. Increase child safety measures
27. Aesthetic appearance of neighborhoods (cameras, etc.)
28. Technology ahead of legal constraints

## APPENDIX C

### LIST OF EVENTS

1. Terrorist Attacks - September 11, 2001
2. Los Angeles riots
3. Super Bowl 2001
4. Another major terrorist event
5. Supreme Court decision – civil liberties
6. Collecting information on political persons
7. Biometric identification of known terrorist/criminal
8. Failure of government to act upon terrorist threat
9. First major lawsuit due to system failure
10. Wrongful conviction using biometrics
11. New biometrics standards approved
12. Failure to attack due to system failure
13. Facial technology – misuse of biometrics
14. Deployment of facial recognition
15. Biometrics proven unreliable – (facial recognition)
16. Supreme Court decision – denies facial recognition technology
17. National I.D. system
18. National TWIC (Transportation Worker I.D. Card)
19. Health hazards due to technology

## ENDNOTES

---

<sup>1</sup> Night Fell on a Different World. (2002, September 7). The Economist, p.22.

<sup>2</sup> Ibid.

<sup>3</sup> Ibid.

<sup>4</sup> Swanbrow, D. (2002, May). "Homeland Insecurity: Survey Shows Many Americans Still Worried and Shaken". UM News. Internet. <http://www.umich.edu/2newsinfo/released/2002/may02/r050302a.html>. Accessed: 6 February 2003.

<sup>5</sup> Ibid

<sup>6</sup> Ibid

<sup>7</sup> Ibid

<sup>8</sup> Ibid

<sup>9</sup> Seffers, G. "How Biometrics Works." Federal Computer Week . April 2002. Internet. <http://www.fcw.com/fcw/articles/2001/0430/pol-biobox-04-03-01.asp>. Accessed: 13 December 2002.

<sup>10</sup> Reedman, C. "Biometrics and Law Enforcement " November 2001. Personal view of the role that biometrics may play in the near and long-term future of law enforcement. Distributed at Biometric Conference, 11 November 2002, Waikiki Beach, Hawaii, (quoted with the author's permission).

<sup>11</sup> Ibid.

<sup>12</sup> Ibid.

<sup>13</sup> Bonsor, K. "How Facial Recognition Systems Work." Internet. <http://computer.howstuffworks.com/facial-recognition.htm>. Accessed: 16 December 2002.

<sup>14</sup> Ibid.

<sup>15</sup> "Face Recognition." Gaits Technology. Internet. <http://www.gaits.com/biometrics-face.asp>. Accessed: 2 December 2002.

<sup>16</sup> Ibid.

<sup>17</sup> Ibid.

<sup>18</sup> "Technology." Internet. <http://www.viisage.com/technology.htm>. Accessed: 2 December 2002.

<sup>19</sup> "Face Recognition," Gaits Technology. Internet. <http://www.gaits.com/biometrics-face.asp>. Accessed: 2 December 2002.

<sup>20</sup> Bonsor, K. "How Facial Recognition Systems Work." Internet. <http://computer.howstuffworks.com/facial-recognition.htm>. Accessed: 16 December 2002.

<sup>21</sup> Ibid.

- 
- <sup>22</sup> Atick, J. "Biometrics: The Technology Review Ten". An MIT Enterprise Technology Review. 1. Internet. <http://www.technologyreview.com/articles/tr10-atick0101.asp>. Accessed: 1 March 2003.
- <sup>23</sup> "Is the U.S. Turning Into a Surveillance Society?" ACLU, web site. Internet. <http://www.aclu.org/Privacy/Privacylist.cfm?c=39>. Accessed: 1 March 2003.
- <sup>24</sup> Ibid.
- <sup>25</sup> Ibid.
- <sup>26</sup> Ibid.
- <sup>27</sup> Matthews, W. "Privacy still a Priority, Officials Say." Federal Computer Week. July 2002. Internet. <http://www.fcw.com/print.asp>. Accessed: 12 February 2002.
- <sup>28</sup> Drummond, D. "Restraints shelved on facial-recognition." The Washington Times. March 2002. Internet. <http://asp.washtimes.com/printarticle.asp?action=print&ArticleID=20020305-14688454>. Accessed: 13 January 2002.
- <sup>29</sup> Whaler v. Roe 429 U.S 589, 605 (1977).
- <sup>30</sup> Woodward, J. Jr., "Super Bowl Surveillance: Facing Up To Biometrics." Rand Study; Arroyo Center. May 2001.
- <sup>31</sup> United States v. Dionisio, 410 U.S 1,14 (1973).
- <sup>32</sup> "Super Bowl Surveillance," Rand Study.
- <sup>33</sup> Ibid.
- <sup>34</sup> Ibid.
- <sup>35</sup> Swanbrow, D. "Homeland Insecurity: Survey Shows Many Americans Still Worried and Shaken." UM News. May 2002. Internet. <http://www.umich.edu/2newsinfo/released/2002/may02/r050302a.html>. 6 February 2002.
- <sup>36</sup> Ibid.
- <sup>37</sup> McCullagh, D. & Zarate, R., "Scanning Tech a Blurry Picture." Wired News. February 2002. Internet. <http://www.com/news/politics/0,1282,50470,00>. Accessed: 23 January 2003.
- <sup>38</sup> "Data on Face-Recognition Test at Palm Beach Airport Further Demonstrates Systems' Fatal Flaws." ACLU Press Release May 14, 2002. Internet. <http://ACLU.org/privacy/privacy.cfm?ID=10340&c=130&Type=s>. Accessed: 2 February 2003.
- <sup>39</sup> Bray, H. "Face Testing at Logan is Found Lacking." The Boston Globe. July 17, 2002. Internet. <http://www.boston.com/dailyglobe2/198/html>. Accessed: 16 December 2002.
- <sup>40</sup> Weil, N. "Fighting Terrorism Without Sacrificing Privacy." IDG News Service. February 2002. Internet. <http://www.pcworld.com/news/article/0,aid,107159,00.asp>. Accessed: 10 January 2003.
- <sup>41</sup> Ibid.
- <sup>42</sup> FRVT Homepage, Face Recognition Vendor Test, Internet. <http://www.frvt.org/>. Accessed: 10 February 2003.

- 
- <sup>43</sup> Preliminary Report Bill Lockyer, Attorney General, Crime 2002 California: 2003.
- <sup>44</sup> Ibid.
- <sup>45</sup> Bonner, J. "Looking for Faces in the Super Bowl crowd." Access Control and Security Systems Integration. March 2001: v.44 no3 P.1, 14-18.
- <sup>46</sup> Kilgannon, C. "Cameras to Seek Faces of Terror in the Vistors to the Statue of Liberty." New York Times, 25 May 2002. Internet. <http://www.nytimes.com/2002/05/25/nyregion/25CAME.html>. 16 February 2003.
- <sup>47</sup> "Super Bowl Surveillance," Rand Study.
- <sup>48</sup> Ibid.
- <sup>49</sup> Arnold, J. "Facial Recognition Streamline Police Services." Governments West January 2003:14-15
- <sup>50</sup> Ibid.
- <sup>51</sup> Ibid.
- <sup>52</sup> Mr. Raymond E. Foster, Lieutenant Los Angeles Police Department, interviewed by author 12 November 2002, Honolulu, Hawaii.
- <sup>53</sup> Vonderheid, E. "Biometrics Verify Travelers' Identity." The Institute, January 2002. Internet. <http://www.spectrum.ieee.org/INST/jan02/fbio.html>. Accessed: 2 November 2002.
- <sup>54</sup> Ibid.
- <sup>55</sup> Hardy, M. "Group Issues Final Biometric Report." FCW.COM, 25, February 2003. Internet. <http://www.fcw.com/print.asp>. Accessed: 30 February 2003.
- <sup>56</sup> Ibid.
- <sup>57</sup> John P. Kotter, Leading Change. Harvard Business School Press, 1996.

---

## BIBLIOGRAPHY

- Arnold, J. "Facial Recognition Streamline Police Services". Governments West, p.14-15, January 2002.
- Atick, J. "Biometrics: The Technology Review Ten". 2001. Internet. <http://www.technologyreview.com/articles/tr10-atick0101.asp>; Accessed: 1 March 2003.
- "Data on face-Recognition Test at Palm Beach Airport Further Demonstrates Systems' Fatal Flaws". Internet. <http://ACLU.org/privacy/privcy.cfm>; Accessed: 2 February 2003.
- Bonner, J. (2001) "Looking for Faces in the Super Bowl Crowd." Access Control and Security Systems Integration no3, 14-18.
- Bonsor, K. "How Facial Recognition Systems Work." 2002. Internet. <http://www.howstuffworks.com/facial-recognition1.html>; Accessed: 16 December 2002.
- Bray, H. "Face Testing at Logon is Found Lacking." The Boston Globe. June 17, 2002. Internet. <http://www.pcworld.com/news/article/0,aid,107159,00.asp>; Accessed 16 December 2002.
- Drummond, D. "Restrains Shelved on Facial-Recognition". 2002. Internet. <http://asp.washtimes.com/printarticle.asp?action=print&ArticleID=20020305-14688454>; Accessed: 13 January 2002.
- "Face Recognition Vendor Test". FRVT Homepage. Internet. <http://frvt.org>; Accessed: 10 February 2003.
- "Face Recognition," Gaits Technology. Internet. <http://www.gaits.com/biometrics-face.asp>. Accessed: 2 December 2002.
- Hardy, M. "Group Issues Final Biometric Report." FCW.COM. February 23, 2003. Internet. <http://www.fcw.com/print.asp>. Accessed: 30 February 2003
- "Is the U.S. Turning Into a Surveillance Society?" Internet. <http://www.aclu.org/Privacy/Privacylist.cfm?c=39>; Accessed: 1 March 2003.
- Kilgannon, C. "Cameras to Seek Faces of Terror in the Visitors to the Statue of Liberty." New York Times, May 25, 2002, p10. Internet. <http://www.nytimes.com/2002/05/25/nyregion/25CAME.html>. Accessed: 16 February 2003.
- Kopper, J. Leading Change. Harvard Business School Press. 1996.

---

Matthews, W. "Privacy Still a Priority, Officials Say". Federal Computer Week, June 2002, Internet. <http://www.fcw.com/fcw/articles/2002/0729/pol-priv-07-29-02.asp>. Accessed 12 February 2003.

McCullagh, D. & Zarate, R., "Scanning Tech a Blurry Picture". Wired News, February 2002. Internet. <http://www.com/news/politics/o,1282.50470,00>. Accessed: 23 January 2003.

"Night Fell on a Different World". The Economist, p.22. 7 September 2002.

Preliminary Report Bill Lockyer, Attorney General, Crime 2002 California: March 2003.

Reedman, C. "Biometrics and Law Enforcement; Personal View of the Role that Biometrics May Play in the Near and Long-Term Future of Law Enforcement". Distributed at Biometric Conference, 11 November 2002, Waikiki Beach, Hawaii, (quoted with the author's permission).

Seffers, G., "How Biometrics Works". Federal Computer Week. April 2002. Internet. <http://www.fcw/articles/2001/0430/pol-biobox-04-03-01.asp>. Accessed 13 December 2002.

Swanbrow, D. "Homeland Insecurity: Survey Shows Many Americans Still Worried and Shaken". UM News, May 2002. Internet. <http://www.umich.edu/2newsinfo/released/2002/may02/r050302a.html>. Accessed: 6 February 2003.

"Technology," Viisage (Face Recognition Advantages), Web site. Internet. <http://www.viisage.com/technology.htm>. Accessed: 2 December 2002.

Vonderheid, E. "Biometric Verify Travelers' Identity." The Institute. January 2002. Internet. <http://www.spectrum.ieee.org/INST/jan02/fbio/html>. Accessed 2 November 2002.

Weil, N. "Fighting Terrorism Without Sacrificing Privacy". IDG News Service. November 2002. Internet. <http://www.pcworld.com/new/article/o,aid,107159,00.asp>. Accessed 10 January 2003.

Whaler v. Roe 429 U.S 589, 605 (1977).

Woodward, J. Jr., (May 2001). "Super Bowl Surveillance: Facing Up To Biometrics". Rand Study; Arroyo Center.

United States v. Dionisio, 410 U.S 1,14 (1973).