NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

MITIGATE SOFT TARGET'S VULNERABILITY AND PREVENT CRIME THROUGH BIOMETRICS

by

Vincent J. Collins

December 2013

Thesis Co-Advisors: Nadav Morag
Paul Smith

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE MITIGATE SOFT TARGET'S VULNERABILITY AND PREVENT CRIME THROUGH BIOMETRICS		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Vincent J. Collins			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U. S. Government. IRB Protocol number _____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

Identifying a known criminal or terrorist, and providing protection for soft targets, is not only the concern of New York City, but of law enforcement agencies and municipalities throughout the country. The research reveals several challenges that may arise in utilizing facial recognition and behavioral recognition technology in closed circuit television systems. In recognizing these challenges, the writer looks to mitigate the vulnerability and prevent crime. The research indicates that the projects' success increased when the environment was controlled. Data sources reviewed show that camera angles or lighting are two factors that can impact the environment control. The thesis also looked at the accuracy of the system and legality of any privacy concerns, as well political, public and media influence may have on an emerging technology system.

Biometric emerging technology surveillance is an industry that is rapidly growing in both the public and private sector. However, It lacks the monitoring of one central authority to insure civil liberties are safeguarded. The research expanded on a Closed Circuit Television (CCTV) system that is currently in place and devises a system that will be the foundation for the future of law enforcement by integrating biometric technology into a security surveillance system.

14. SUBJECT TERMS Closed Circuit Television, Facial Recognition, Behavioral Recognition, Soft Target, Central Authority			**15. NUMBER OF PAGES** 97
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

MITIGATE SOFT TARGET'S VULNERABILITY AND PREVENT CRIME THROUGH BIOMETRICS

Vincent J. Collins
Lieutenant, New York City Police Department
B.A., Saint John's University, 1988
M.P.A., Marist College, 2005

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2013

Author: Vincent J. Collins

Approved by: Nadav Morag, PhD
Thesis Co-Advisor

Paul Smith
Thesis Co-Advisor

Mohammed Hafez, PhD
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Identifying a known criminal or terrorist, and providing protection for soft targets, is not only the concern of New York City, but of law enforcement agencies and municipalities throughout the country. The research reveals several challenges that may arise in utilizing facial recognition and behavioral recognition technology in closed circuit television systems. In recognizing these challenges, the writer looks to mitigate the vulnerability and prevent crime. The research indicates that the project's success increased when the environment was controlled. Data sources reviewed show that camera angles or lighting are two factors that can impact the environment control. The thesis also looked at the accuracy of the system and legality of any privacy concerns, as well what political, public and media influence may have on an emerging technology system.

Biometric emerging technology surveillance is an industry that is rapidly growing in both the public and private sectors. However, it lacks the monitoring of one central authority to ensure civil liberties are safeguarded. The research expanded on a Closed Circuit Television (CCTV) system that is currently in place and devises a system that will be the foundation for the future of law enforcement by integrating biometric technology into a security surveillance system.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

NYPD	New York City Police Department
CCTV	Closed Circuit Television
LMSI	Lower Manhattan Security Initiative
LPR	License Plate Reader
LDA	Linear Discriminant Analysis
PCA	Principal Component Analysis
EBGM	Elastic Bunch Graph Matching
FERET	Facial Recognition Technology
FRVT	Facial Recognition Vendor Testing
HMM	Hidden Markov Method
CAT	Combat Auto Theft
RISS	Regional Information Sharing System
VBIED	Vehicle Bourne Improvised Explosive Device
FOIL	Freedom of Information Act
ACLU	American Civil Liberties Union

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The intention of this thesis was to create a policy that can maximize the effectiveness of closed circuit television (CCTV) systems by utilizing facial recognition and behavioral recognition software in a proactive manner to both mitigate soft targets' vulnerabilities and prevent crime.

Soft targets are difficult to protect, but there may be a way to mitigate this vulnerability by detecting pre-attack operational surveillance on the part of terrorists or criminals through the advances in emerging technology, such as facial recognition and behavioral recognition technology. Real-time surveillance would not only provide the ability to detect action before an attack or crime occurs, but it would be able to provide actionable intelligence to security and law enforcement personnel to respond to an attack or crime that is unfolding. It may also provide the ability to disrupt a future attack or criminal incident and limit causalities of an attack or victims of a crime. Soft targets are types of locations that have historically been susceptible to both criminal and terrorist activity. Whether it is a terror bombing of a nightclub or housing complex, or a shooting at a shopping mall or movie theater, all of these locations are prone to both terror and criminal incidents. Closed circuit television systems can provide mechanisms to resolving the vulnerability at these targets, but emerging technologies can provide an enhanced layer of protection.

The solution to the vulnerability will be found in an analysis of case studies. Facial recognition technology was implemented with CCTV surveillance systems in Virginia Beach, Ybor, Florida, at the 2001 Super Bowl and in Newham, England. A case study review of these projects' successes and failures was conducted in order create a more effective viable system.

The analysis and conclusion centers on four elements researched on this matter. The four elements are the technology, deployment of cameras, monitoring and use of personnel and legal political ramifications. The research started out as an effort to see if the technology was ready to operate in a proactive manner, as opposed to the reactive

forensic manner in which the technology is currently used. Although there will continue to be the need to utilize the technology in a forensic manner, the research has shown that surveillance systems, such as closed circuit television and emerging technologies like facial recognition and gait recognition can enhance security.

There are legal, privacy, media and political concerns the research clarified, and the final recommendation of the development of a central authority will provide the resolution to these questions.

ACKNOWLEDGMENTS

"As we express our gratitude, we must never forget that the highest appreciation is not to utter words but to live them." —John Fitzgerald Kennedy

There are so many people that words cannot express the gratitude I have for the role they have played in completing this work. Dr. Nadav Morag and Professor Paul Smith, my thesis advisors, thank you so much for your guidance, encouragement and support of this work.

Another acknowledgement of gratitude must be extended to the New York City Police Department and our Commissioner the Honorable Raymond W. Kelly, who allowed me the opportunity to study at this prestigious program.

I would also like to thank my sister Anne Marie, who always offered her editing expertise or thoughtful word on a moments notice. My sister Kathy was always available to pitch in while I was away. Mom and Dad, what can I say about a lifetime of reassurance that you both have always provided.

The final gratitude goes to my lovely wife, Terry, who stood by my side throughout this process, gave her unwavering support, and watched over our four beautiful children while I dedicated time to this work. You lived those words of gratitude and I am forever grateful.

I would like to dedicate this work to all those we lost that fateful day, September 11, 2001, as well as to all those who still place themselves in harm's way. Be Safe!

THIS PAGE INTENTIONALLY LEFT BLANK

I. PROBLEM STATEMENT

When a person walks into any police precinct in New York City or someone accesses the new NYPD I-phone application, he will see posters of wanted individuals and missing persons. The posters are visibly displayed so that officers going on patrol or citizens visiting the location both have access and can assist with identifying either wanted or missing individuals. In some cases, the media is utilized to get the message out to the public. In all cases, law enforcement is relying on the keen eye or intuition of private citizens and officers to recognize the individual. Although the keen eye of citizens is a necessary tool in combating both crime and terrorism, emerging technologies such as facial recognition and behavioral recognition can replace the dependency on the individual citizen. It should be noted that crime prevention is not the only aspect of concern. Soft targets are a recognized vulnerability that can be protected by emerging technologies. The concern of identifying a known criminal or terrorist, and in doing so creating a system that will provide protection for soft targets, is not only the concern of New York City. Law enforcement agencies and municipalities throughout the country face similar problems.

A. INTRODUCTION

The intention of this thesis will be to create a policy that can maximize the effectiveness of closed circuit television systems by utilizing facial recognition and behavioral recognition software in a proactive manner to both mitigate soft targets' vulnerabilities and prevent crime.

In a May 6, 2006, article for the *Washington Pos*t, Clark Kent Ervin discussed how government facilities are more secure since September 11, 2001. In the article, Ervin stated that securing government facilities has "increased the appeal of shopping malls, sports arenas, hotels, restaurants, bars, nightclubs, movie theaters, housing complexes and other 'soft' targets that remain relatively unprotected against terrorist attacks."[1] Soft

[1] Clark Kent Ervin, "Terrorism," *Washington Post*, May 6, 2006, Weekend Edition, 19 Nov. 2013, http://www.washingtonpost.com/wp-dyn/content/article/2006/05/05/AR2006050501754.html.

targets have repeatedly been a concern to policy makers. They are a known vulnerability with limited physical protection in some cases. Soft targets are generally opened, accessible and unprotected by their very nature. In most cases, soft targets are privately owned and dependent on the security of the property owner.

Soft targets are difficult to protect, but there may be a way to mitigate this vulnerability by detecting pre-attack operational surveillance on the part of terrorists or criminals through the advances in emerging technology, such as facial recognition and behavioral recognition technology. Real-time surveillance would not only provide the ability to detect action before an attack or crime occurs, but it would be able to provide actionable intelligence to security and law enforcement personnel to respond to an attack or crime that is unfolding. It may also provide the ability to disrupt a future attack or criminal incident and limit causalities of an attack or victims of a crime. Soft targets are types of locations that have historically been susceptible to both criminal and terrorist activity. Whether it is a terror bombing of a nightclub or housing complex, shooting at shopping mall or movie theater, all of these locations are prone to both terror and criminal incidents. Closed circuit television systems can provide mechanisms to resolving the vulnerability at these targets, but emerging technologies can provide an enhanced layer of protection.

In order to use these emerging technologies, it requires integration with a system that has been used for security protection for decades. Closed circuit television (CCTV) systems can provide the platform for security and law enforcement personnel to integrate these emerging technologies. One of the first closed circuit television systems in the United States was installed at a Sears Department store in Olean, New York, in September 1968.[2] The Olean Sears store allowed the closed circuit television system to be monitored by the Olean Police Department. Olean was not only one of the first retail surveillance systems, but it also created one of the first public-private partnerships in surveillance systems. The strategy was devised to prevent crime. Over the years the

[2]"Back to Basics: Where Did the Video Security System Come From?," *Security Articles and News VinTech Systems*, n.d., http://www.vintechnology.com/journal/uncategorized/back-to-basics-where-did-the-video-security-system-come-from/, 19 Nov. 2013.

private sector companies advanced in their use of the technology in order to improve their loss-prevention methods. The need to build public and private partnerships to augment security will need to be addressed in the policy. Since September 11, 2001, many municipalities in the United States have integrated closed circuit television systems in an effort to prevent crime and protect against terrorism. Unfortunately, a majority of these systems do not have the manpower to monitor cameras twenty-four hours a day. In the United Kingdom, closed circuit television systems have been successfully operated and expanded on since the 1990s. The British system is centrally regulated and controls private and public CCTV systems through the Data Protection Act. The British system regulates the surveillance system from the collection and storage of data to licensing of security personnel who operate the system. The British system may have some of the answers, but not all of them. Security personnel who are licensed and trained in operating the CCTV system provide a comfort level of professionalism to both the agency utilizing the system and the public. What they do not provide is the ability to monitor every camera. There is no definitive number of personnel who could be hired to effectively cover all operational cameras. It is essential to have an expansive camera system but also necessary that emerging technologies are utilized to insure the efficiency of the system. These are all issues to be considered in a policy development.

The studies conducted on closed circuit television regarding crime prevention efforts in the United States have been inconclusive in clearly delineating if there is a correlation between crime prevention and surveillance systems.[3] Many municipalities throughout the United States have attempted to adopt closed circuit systems similar to those that have evolved in Great Britain.

In New York City, closed circuit television systems have proliferated and improved throughout the last decade. In Lower Manhattan, thousands of cameras monitor everyday activity throughout the city. On August 8, 2012, the New York Police Department announced that their new Domain Awareness System was operational. The Domain Awareness System was a joint venture with Microsoft Corporation, but both

[3] Rajiv Shah and Jeremy Braithwaite, "Spread too Thin: Analyzing the Effectiveness of the Chicago Camera Network on Crime," *Police Practice and Research* (forthcoming) (2012): 1–13.

parties clearly noted that facial recognition software was not employed in this joint venture. It should be pointed out that the New York City Police Department does utilize facial recognition software in criminal investigation but not in their new surveillance system.[4] Currently, the New York City Police Department uses facial recognition technology strictly as a forensic investigative tool in a similar fashion to closed circuit television. Investigators currently use facial recognition technology and closed circuit television systems as a tool in a post incident investigation, in order to build or enhance a case.

The Lower Manhattan Security Initiative (LMSI) is part of the Domain Awareness System. It has instituted a closed circuit television surveillance that is similar in scope to the "Ring of Steel," which is the video surveillance system that protects the City of London. The current New York City surveillance system utilizes license plate readers in order to identify vehicles that are stolen or the subject of a criminal investigation. The license plate reader model will provide the platform to expand the emerging technologies system, but using this strategy will create the need to devise an alert procedure to make positive recognition notifications.

The primary reason for graduate research on this topic is to expand on a CCTV system that is currently in place and devise a system that will be the foundation for the future of law enforcement by integrating facial recognition technology. There are lessons that can be learned from the implementation of surveillance systems throughout the country utilizing emerging technology. The technology provides a nonintrusive method with the ability to scan millions of faces in a public place in seconds. There is no amount of personnel who could physically participate in such a project. This technology increases law enforcement's ability to conduct surveillance in the public form and should greatly improve security. It will allow the opportunity to identify individuals before they will act. Facial recognition, if properly implemented, will be able to improve law enforcement deployment by focusing security where facial recognition alerts occur.

---

[4] Rocco Parascandola, "NYPD Planning to Use Facial Recognition Technology to Match Mug Shots to Suspect Videos," *NY Daily News (*Mortimer Zuckerman) 5 Feb. 2011, http://www.nydailynews.com/new-york/nypd-planning-facial-recognition-technology-match-mug-shots-suspect-videos-article-1.136071.

B. RESEARCH QUESTION

How can the New York City Police Department construct a policy that will integrate facial recognition technology in a closed circuit video surveillance system in a cost effective nonintrusive way in order to identify suspicious criminal individuals and possible terrorists? Can integrating this technology mitigate soft target's vulnerability? Can this system provide a paradigm for the future of surveillance systems?

C. LITERATURE REVIEW

The purpose of this review is to form the building blocks of a thesis that will discuss the operational and legal issues of implementing facial and behavioral technology in soft target protection. The literature will be broken down into three components. The first of these components will look at literature on Biometric facial recognition technology. The second component will review literature that focuses on and shows a direct correlation between the use of CCTV systems and law enforcement. The third literature component will discuss the intelligence cycle and where the use of this technology will fit into the cycle.

1. Literature on Biometric Facial Technology

One of the initial articles reviewed discussed the use of biometric facial technology as an investigative tool at the 2001 Super Bowl in Tampa Bay, Florida. John D. Woodward, Jr. is the author of the Super Bowl Surveillance report "Facing Up to Biometrics" and has authored, as well as participated in numerous lectures, on the Biometric technology subject. The technology was implemented as cutting edge technology at the time. The author points out that the system was used to prevent crime, as well as a terrorist attack at a large spectator event. Woodward immediately addresses the glaring issue, "privacy." He answers and asks the question on whether society should be concerned. The author cites numerous examples in the private sector and foreign countries where the technology is successfully used. Woodward, an attorney, astutely describes the civil libertarian's concern but cites that there is no reasonable expectation of privacy in a public venue. The author does cite potential privacy concerns as the

technology advances. Two of the privacy concerns are the "tracking" and "clandestine capturing" of images that would allow an individual to identify locations a person has visited over the past month.

It must be taken into account that this article was written prior to the September 11, 2001, attacks and before investigators realized that terrorist organizations conducted surveillance of prospective targets. Woodward realized the potential of the technology and also realized the necessity to safeguard privacy of the individuals. The technology used at the 2001 Super Bowl was considered largely successful primarily because there was no terrorist attack at the event. It would be difficult to determine if the event was protected by the new technology or simply by making it known that such technology existed. This information alone may deter any action on the part of a terrorist organization. In the Super Bowl event, facial images were taken at the entry checkpoint into the venue and the still digital images were compared to known digital images.

Kelly Gates, a professor of communications at the University of San Diego, published a book entitled *Our Biometric Future-Facial Recognition Technology and Culture of Surveillance*. In Gates' book, published in 2011, she gives a history of Biometric technology and the development of this technology. Gates is skeptical of the identification process and breaks down the scientific technology. Gates shows the complexity of the technology and specifically cites the use of the technology by the Ybor Police Department outside Tampa Bay, Florida. She points out that the technology could not successfully identify criminals and was subsequently removed.[5]

One of the initial public locations to utilize the technology in a crime-fighting capacity was in Newham, England. In 1997, the United States company Visionics installed the technology on cameras in Newham. Visionics, which today is now known as Morpho Trust USA, still drives the private sector movement toward the use of this technology. Gates does not have a substantial discussion about Newham implementation of the technology. She looks to other socio-economic factors that can be attributed to crime reduction and is not able to definitively connect the reduction to the technology.

[5] Kelly Gates, *Our Biometric Future-Facial Recognition Technology and the Culture of Surveillance* (New York City: New York University Press), 2011.

The Rand Corporation conducted a study for the Virginia State Crime Commission in 2003, as counties within Virginia prepared to use this technology. Virginia Beach applied the technology examined in the Rand report and in 2007 discontinued the use of the system. "To the department's surprise, the system began sounding up to 300 alarms a night. To its annoyance, all of the supposed matches were quickly found to be no match at all." [6] Woodward's initial report about the Super Bowl Surveillance mentioned the concern of "the danger that the biometric facial recognition system will make an incorrect match."[7]

"Biometrics: A Look at Facial Recognition" was a brief prepared by John Woodward, Christopher Horn, Julius Gatune, and Aryn Thomas. The brief was prepared to educate the Virginia State Assembly about biometric technology, so it could be made available to law enforcement in Virginia. The article gives a quick overview of what types of biometric technology exist and more specifically addresses facial recognition technology. The brief also looks at the technology from a legal standpoint and takes into account constitutional issues. The brief cites that facial recognition software provides the ability to locate missing children, terrorists and criminals. The authors cite the nonintrusive nature of the technology as a positive reason to use it. The authors express concern about the human factor in facial recognition and note that the software will not tire or just simply stop paying attention. In a similar manner to the previous article, the authors see the potential of the technology but also see the need for safeguards on the system.[8]

Gates' book opens with the photo of Mohammad Atta, one of the 911 hijackers, standing at a security checkpoint in an airport in Maine. It clearly identifies the reason for

---

[6] Thomas Frank, "Local Agencies Test Sites for ID Software," *USA Today* (10 May 2007), www.itl.nist.gov/iad/news/IDSoftware.html.

[7] John D. Woodward Jr., *Super Bowl Surveillance: Facing Up to Biometrics (*Santa Monica CA: Rand Arroyo Center, 2001), 1–16.

[8] John D. Woodward Jr. et al., *Biometrics: A Look at Facial Recognition* (Santa Monica, CA: Rand Corp, 2003), 1–25.

implementing such a technology, but when law enforcement continually reviews how the technology is used in the public sector locations throughout the country, failure is often the result.

In a Toronto Star article earlier this year, Gates stated that, "eye and facial recognition technology are predicted to account for nearly $4 billion of the biometric industry's $11 billion in annual revenues by 2017."[9] With limited success stories in the public sector, the question arises regarding where the driving force behind the industry originates. The private sector and the military would seem to be two examples of how the technology is being integrated successfully. The examples that are cited in the private sector can help to establish the building blocks for successful integration in law enforcement practices.

On February 16, 2012, Charles Duhigg, in a *New York Times* magazine article, cited how stores such as Target are using the technology as predictive analytics that can help the company target advertise to customers.[10] Another prodigious industry that has successfully implemented the technology is the gambling industry. In Ontario, Canada, digital images are taken of gamblers as they enter the casino, the images are compared to images of gamblers who have been convicted of various casino crimes and are prohibited from entering the casino. It takes seconds to advise the customer whether he or she can enter or not.[11] An article on Biometrics Magazine quoted Otto Wulferding, managing director of Spielbank Hamburg, as saying "Implementing biometrics has made Casino Esplanade substantially safer, in addition to helping us identify banned gamblers more quickly. [12] The private sector success stories may have answers to whether the technology can effectively be integrated into an intelligence paradigm for security.

---

[9] Jim Spencer, "Facial Recognition Is Becoming Big Business," *Star Tribune*, 26 Aug. 2012, http://www.startribune.com/business/166593666.html.

[10] Charles Duhigg, "How Companies Learn Your Secrets," *New York Times*, August 17, 2012.

[11] Dan Robson, "Facial Recognition a System Problem Gamblers Can't Beat?" Thestar.com. 12 Jan 2011, http://www.thestar.com/news/gta/2011/01/12/ facial_recognition_a_system_problem_gamblers_cant_beat.html, Star Tribune.

[12] Mark Lockie, "NBSP to Commence Testing Programme," *Biometric Technology Today (*2006).

On October 8, 2012, the Wall Street Journal published an article written by Ramstad Evans. The article was titled "Big Brother at the Mall." The article showed how facial recognition technology was being utilized at kiosks in shopping malls to identify customers and target advertising toward them.

A recent Congressional Research report discussing the use of drones in domestic surveillance cited how the military utilizes facial recognition technology in drone surveillance. The report also cited Supreme Court cases that would advocate aerial surveillance either by drone or stationary location based on the premise that the threshold for the expectation of privacy was significantly lower in a public area.[13]

The United States Senate Judiciary Subcommittee on Privacy, Technology and the Law conducted a hearing on July 18, 2012. The final article reviewed was from a July 18, 2012, subcommittee meeting in which facial recognition technology and privacy implications were debated. The article shows the gravity that this issue has on the United States government.

On July 18, 2012, Senator Al Franken, the Chairman of United States Senate Judiciary Subcommittee on Privacy, Technology and the Law chaired a meeting in which facial recognition technology and privacy implications were debated. The meeting looked at the law enforcement and Justice Department concerns but the prevailing issue was the infringement on individual liberties. Senator Franken opened the meeting by stating "I want to be clear: there is nothing inherently right or wrong with facial recognition technology. Just like any other new and powerful technology, it is a tool that can be used for great good. But, if we do not stop and carefully consider the way we use this technology, it may also be abused in ways that could threaten basic aspects of our privacy and civil liberties."[14]

---

[13] Richard M Thompson, "Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses," Congressional Research Service, Library of Congress, 2012.

[14] Senator Al Franken, "What Facial Recognition Technology Means for Privacy and Civil Liberties." *View a Hearing or Meeting*. Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law, 18 July 2012.

The subcommittee hearing covers all aspects of the deployment of biometric technology in private and public sectors. Experts spoke on how the technology continues to evolve. The subcommittee concluded with a staff attorney from the Electronic Frontier Foundation expressing concern over information sharing by law enforcement in different jurisdictions.

Woodward would appear to be right. There is tremendous potential with biometric facial recognition technology. It will take a private and public sector partnership in order to successfully integrate the technology. The Lower Manhattan Initiative, which currently is that partnership that the Domain Awareness System has been integrated into what will be the first building block for this project. Missing persons could potentially be found and identity thieves could be stopped before participating in a crime. Sex offenders or violators of orders of protections could be identified outside of locations before they commit heinous acts. The potential for an improving quality of life and identifying potential terrorist does exist.

2. Literature on Closed Circuit Television Surveillance and Law Enforcement

There have been numerous articles and publications written on this subject that has rapidly emerged after September 11, 2001. The most prominent work written about the emerging field surveillance CCTV was written by Clive Norris and Gary Armstrong. The authors wrote *Maximum Surveillance Society: The Rise of CCTV*, and they give both a historical perspective and anthology of the use of video surveillance by law enforcement. Norris and Armstrong focused on the success the British Government had integrating this technology into law enforcement practices. Norris and Armstrong did point out "the exponential increase in visual surveillance creates a massive and costly problem of information processing and handling. [15] License Plate Reader, more commonly known as LPR, was also discussed as a technology that has been integrated with the video surveillance system. LPR's success is another example of the need to

[15] Clive Norris and Gary Armstrong, "*The Maximum Surveillance Society: The Rise of CCTV,"* Oxford: Berg, 1999, 210.

utilize the technology on the person as opposed to the property. The authors spoke of facial recognition as the future direction that the video surveillance field would move toward.

Another publication "Best Practices of Video Evidence Surveillance" focused on the physical structure of the technology and the proper implementation to insure maximum effectiveness as an evidentiary tool.[16] When creating a CCTV system that integrates facial recognition technology, there should be an anticipation of the inevitable litigation that could occur with a criminal prosecution based on the technology integration. It is imperative that best practices are implemented from the outset.

The British Home Office conducted a study known as "Assessing the Impact of CCTV." The British study was authored by Angela Spriggs and Martin Gill and was critical of the funding of an elaborate CCTV system, but felt it was also necessary venture. The study was conducted for the Parliament in order to inform the British people how their CCTV system was working. Although there are limited studies of CCTV systems in the United States, none of these studies show the same sense of transparency.

An additional study was lead by Brandon Welsh and David Farrington on "Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta Analysis." Their work focuses on CCTV systems throughout the world and finds both flaws and successes. By developing this new policy, individuals would use this information to learn from the failures and implement the segments that have made previous systems successful.

Greenberg and Roush's assessment of closed circuit television systems suggested that in order to be successful, closed circuit television must be monitored.[17] Most of the studies showed the increase in cameras as positive aspect of success. An increase in operational cameras will also need to address the ability to monitor. The Greenberg and

---

16 United States, Combating Terrorism Technical Support Office, Technical Support Working Group, *Best Practices for the Retrieval of Video Evidence from Digital CCTV Systems*, Version 1.0. Arlington, VA: Technical Support Working Group, 2006.

17 David F. Greenberg and Jeffrey B. Roush, "The Effectiveness of an Electronic Security Management System in a Privately Owned Apartment Complex," *Evaluation Review* 33, no. 1 (2009): 3–26.

Roush study did not discuss how to provide training and hiring of personnel to adequately staff any surveillance system. This study involved security surveillance at a private apartment complex in New York City. Green and Roush are correct in identifying the need for more cameras. It should also be recognized that by continuously adding more cameras, and personnel to monitor these cameras. Eventually, there will have to be a decision made as to what point to stop because there will never be a point where enough personnel can be hired to monitor all cameras all the time.

3. Literature on the Intelligence Cycle

When creating a system that will develop facial recognition technology through CCTV, it must be understood that the data collected will be filtered through the intelligence process. Mark Lowenthal in his book "Intelligence from Secret to Policy" points out much more intelligence is collected than can ever be processed and exploited."[18] The general principal of collection, collation, evaluation, analysis and dissemination would apply. In cities such as New York and London, systems are already in place to alert 911 or other intelligence services, depending on the circumstances, of the alert that is generated under video surveillance. "The common almost reflexive initial reaction to intelligence failures is to see them as results in deficiencies in collection." [19] Facial recognition technology with the ability to view millions of faces in seconds will increase the data collected but will also increase the efficiency. No excuse, in the future, will be acceptable when video feeds are used for forensic evidence, and that same technology existed to stop an attack or criminal act before it occurred.

4. Conclusion

In an effort to balance the freedom of the individual and public safety, the Literature Review focused on the emerging technologies facial and behavioral recognition technology. The purpose of this focus is to analyze whether it is feasible to integrate these systems to provide both public safety and protection. There are disparities

[18] Mark M Lowenthal. *Intelligence: From Secrets to Policy*. Los Angeles: SAGE/CQ, 2012. Print.

[19] Jennifer E Sims and Burton L. Gerber. *Transforming U.S. Intelligence*. Washington, D.C.: Georgetown UP, 2007. Print.

that need to be considered in order to integrate such a system. The accuracy of the system and legality of any privacy concerns are at the forefront of these disparities. The political, public and media influence are additional concerns an integration of this system. In the analysis where the systems were initially integrated, political, public and media ramifications were not addressed in the literature.

5. Methodology

The New York City Police Department currently utilizes CCTV systems in surveillance of the Financial District, Midtown Manhattan and other critical infrastructures throughout the city. The object of this study will be to integrate facial recognition technology into the current system.

Facial recognition technology is an emerging technology that recently is shown to be effective in identifying faces in a crowd. The primary method of data analysis in this thesis will be a case study of prior projects that have utilized this technology. In order to determine their capabilities and effectiveness, the study would like to use facial recognition technology to identify individuals on a terrorist watch list or wanted poster who travels through the targeted area.

The data sources will consist of literature of former studies of how CCTV has been utilized in other jurisdictions, as well as facial recognition technology. The License Plate Reader (LPR) program has applied a similar emerging technology to the use of CCTV. The primary sources of the license plate reader program will be internal reporting. The Combat Auto Theft Program in the 1990s developed public and private cooperation in order to address auto theft. In the Auto Theft Program, participants were provided a decal to place in the window of their car to show they were partaking in the program. The thesis will also look at this program as a method of implementing a more transparent CCTV system. Cooperating private sector businesses would display a similar decal to inform the public that they are under surveillance.[20] The paradigm for future systems will be an intermingling of systems that have previously been used, as well as an

[20] "All New York Getting Car-Theft Decal Plan."*New York Times*. 19 Aug. 1990. Web. 19 Nov. 2013.

analysis of case studies where the technology was implemented. The individual case studies were chosen due to their relevance in integrating an emerging technology system in a metropolitan urban environment. The Super Bowl case study presented a controlled environment. Whether operating the technology in a controlled or opened environment, it was important to analyze all aspects of how the technology can be applied.

The case study analysis will be the method of analysis used to identify a solution to the issue. Facial recognition technology was implemented with CCTV surveillance systems in Virginia Beach, Ybor, Florida, and at the 2001 Super Bowl. A case study review of these projects' successes and failures will be conducted in order create a more effective viable system.

The following steps will be used to judge the success or failure of the program: concern over accuracy of identification and the legal and political privacy. The project will be finished when an effective nonintrusive method of securing public domain is in place. In selecting studies for this project, the research has concentrated on detecting the role that legal and privacy concerns played in decision making. Another aspect concerns whether or not these technologies actually deterred crime and what function the technology essentially had in the investigations of crimes. These case studies will also be viewed from the perspective of how did these municipalities integrating the technology approach and deploy the CCTV cameras.

The final output of the analysis will be a model for how facial recognition technology can be integrated into surveillance systems initially in New York City, and eventually throughout United States, in order to provide a nonintrusive layer of protection to society.

Closed circuit television systems utilizing facial recognition and behavioral recognition software in a proactive manner can mitigate soft target's vulnerability and prevent crime. In order to better understand the role these emerging technologies can play in mitigating vulnerability, we must first look at the technology itself.

This chapter has given an overview of why the research is necessary and outlined some of the parameters and obstacles that will be analyzed in a new surveillance system

utilizing emerging technologies. The subsequent chapter will look at the technology itself and explain what factors will make this technology effective. The chapter will also explain how the technology evolved and describe how this evolution in technology has led to a system that can be applied to a surveillance system.

THIS PAGE INTENTIONALLY LEFT BLANK

II. FACIAL AND BEHAVIORAL TECHNOLOGY

The previous chapter showed an outline of the expectations of this thesis. This chapter will start the process and give an overview of biometric technology while explaining both the history and capability of facial recognition technology, as well as gait recognition technology. Gait recognition is the form of behavioral technology that will help mitigate the soft target vulnerability.

The ability to recognize a person is a difficult task for most and worthy attribute for the individual who can place a name with the face. The ability to scan a crowd of thousands of faces and identify numerous individuals is something that, until recently, would never have seemed possible. It still is not possible with the human eye, but the advances in technology have made what would have seemed impossible more than a reality. Biometric technologies are evolving in a way that make recognition of individuals by their facial features or gait an actuality.

Biometric technology is an emergent field that is currently used in various forms by both the public and private sector. The Merriam-Webster dictionary defines biometric as the measuring of physiological or behavioral characteristics.[21] The word is drawn from an ancient Greek derivative. There are nine recognized forms of biometric technology. The nine forms are broken down into two categories—physiological and behavioral. Fingerprint, hand, iris, retina and facial recognition are all considered physiological forms of biometric. While signature, voice, keystroke and gait recognition are behavioral forms. The physiological biometrics consists of a mathematical algorithm that identifies a specific body part, while behavioral biometric technology focuses on the movement of a specific body part.

Facial and gait will be defined in great detail but a discussion of biometrics would not be complete without an explanation of the other forms that may be more commonly

21 "Biometrics,"*Merriam-Webster,* Merriam-Webster, n.d. Web. 19 Nov. 2013. http://www.merriam-webster.com/dictionary/biometrics.

recognizable. Fingerprint, Hand, Iris, Retina, Signature, Voice and Keystroke are all forms of biometrics that may be readily recognizable.

Fingerprint is a form of identification that has been around for centuries. The fingerprint has innate characteristics that make it a successful method of identification. Law Enforcement has used the fingerprint for identification in criminal cases for over a century. Both the public and private sector have used biometric fingerprint for controlling security access points. On September 10, 2013, Apple introduced the iPhone 5. The phone allows security access through biometric fingerprint.[22] Every day the integration of biometric technology into society continues to advance. In a similar fashion Hand, Iris and Retina biometrics have been developed and are primarily used in a security capacity to monitored access to controlled areas. Facial recognition will use the same physiological forms of biometric identification of individuals by identifying distinct parts of the human body.

Signature is a form of biometric that is often seen when an individual signs an electronic pad after using their credit card. It is very common in today's society yet probably goes unnoticed. Voice recognition and Keystroke recognition are behavioral biometrics that can also be seen actively used in society today. Keystroke is a common method of any computer password access. An easily identifiable example of Voice recognition is more commonly seen on modern smart phones when the operator makes a voice operated request to call someone. All of these technologies whether physiological or behavioral biometrics can be seen in use in various capacities throughout the world.

Facial recognition and gait recognition are the two forms of biometric technology that this thesis will specifically concentrate on to mitigate soft target vulnerability. The rational for focusing specifically on these types of biometrics is their ability to identify specific individuals and the furtive movement of people in a crowd. These are very different types of objectives and precisely why these technologies

[22] Senguta, Somini, "Machines Made to Know You, by Touch, Voice, Even by Heart." "Bits Machines Made to Know You by Touch Voice Even by Heart Comments," *The New York Time*s, 10 Sept. 2013, http://bits.blogs.nytimes.com/2013/09/10/beyond-passwords-new-tools-to-identify-humans/?emc=edit_tnt_20130910.

were chosen to diminish the threat. When mitigating the vulnerability of either a terrorist attack or criminal action, it is necessary to identify suspicious behavior before it develops into action.

Furtive movement is a term often used by law enforcement when describing the actions of an evasive individual who appears to be acting in a suspicious manner. The individual could be a potential robbery suspect conducting surveillance of an area to identify a potential victim. Suspicious behavior could be as simple as an individual lingering around a transportation facility while buses and trains come and go, and the individual chooses not to get on any of them. Whether criminal or terrorist in nature, the individual will attempt to blend into the crowd. Facial recognition possesses the ability to recognize the individual in the crowd, only if this individual is listed in a database of known terrorist or criminal suspects. Gait recognition can identify the gait from an individual as one that has exhibited similar gait behavior previously at the location.

A May 20, 2013, *New York Times* article discussed how Premier League professional soccer teams in England were using facial recognition technology to identify fans who were previously barred from a venue. It allowed the team to provide a safe venue for fans to watch the game.[23] This is only one example of how facial recognition can be used in a modern society.

A. HISTORICAL GENESIS OF FACIAL RECOGNITION

"As facial recognition technologies have become more accurate and less costly, commercial interest and investment in these technologies has grown."[24] Many would say Woodrow Bledsoe, Helen Chan Wolf and Charles Bisson were the initial forerunners in the field of facial recognition. Their studies on the topic began in 1964 with a private research firm in Palo Alto and continued on with Stanford University.[25] The Bledsoe,

---

[23] Sarah Lyall, "In England, Police Tactics Aim to Stop Trouble Before It Starts." *The New York Times* [New York] 20 May 2013: 17.

[24] Sony Corporation, "Sony Corporation Global Headquarters," S*ony Global*, n.d., http://www.sony.net/SonyInfo/technology/technology/theme/sface_01.html.

[25] W. W. Bledsoe and H. Chan, 1965. A Man Machine Facial Recognition System—Some Preliminary Results, Technical Report PRI 19A, Panoramic Research, Inc., Palo Alto, CA.

Chan Wolf and Bisson system compared human faces against still images. Their technology was relying on the operator of the system playing an active role in the identification process. The formulas utilized to assist in the identification were manually entered at various stages in the process. The system was plagued by very similar problems as the systems developed over the years. As the technology and computer technology evolved, this process became automated and controlled by the computer. The angle and lighting of images caused similar inaccuracies over the course of the technologies development.

Now that there is an understanding of how biometric technology came about, the next question would be how does it work? The basics of the technology exist in understanding that there are two core types of algorithms utilized in the technology geometric and photometric. Geometric algorithm is a calculated formula utilized to identify characteristic qualities in the image. Photometric refines an image into mathematical principles. These two initial paradigms evolved into the modern algorithms model that currently identify with the modern facial recognition technology. Over the years, numerous algorithms have been formulated and applied to support the development of facial recognition technology.

Both photometric and geometric algorithms can be explained in Figure 1. The system identifies points on the face, such as nose, eyes and mouth. The distances are measured between these locations and compared to the distance between specific facial points on known faces in the database.

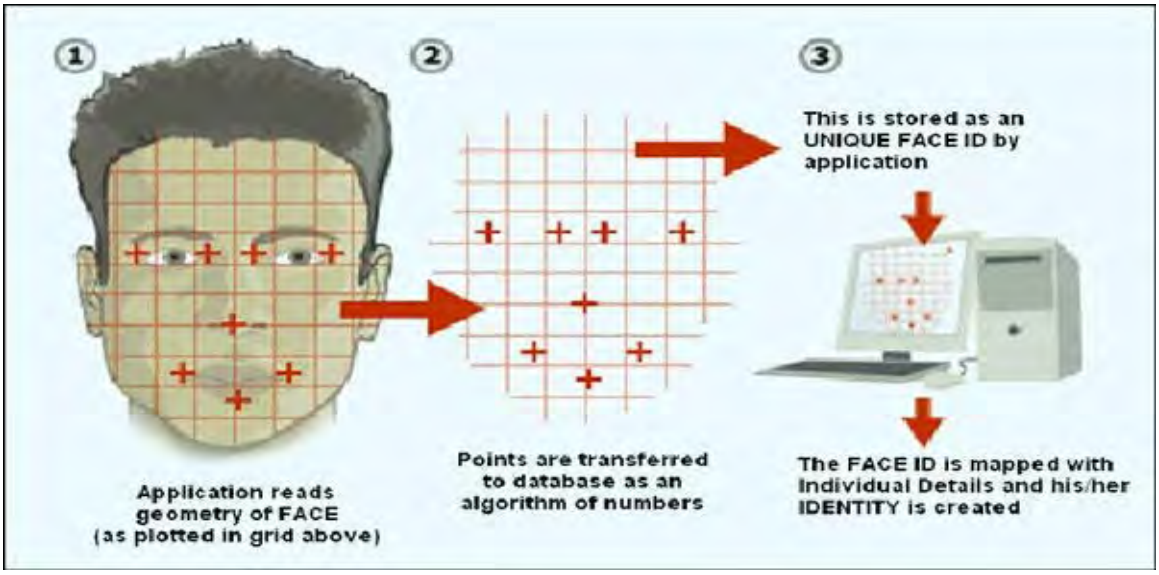

Figure 1. Geometric breakdown of face transferred into algorithm of numbers[26]

This basic format evolved into even more specific indicators, such as the 1971 study by A. J. Goldstein, L. D. Harmon, and A. B. Lesk. They continued the study of facial recognition and devised twenty-one particular indicators, such as hair color and lip thickness, but like Bledsoe's earlier system, the project was reliant on the ability of the operator entering the data.[27] It was still not an automated system and only worked on identifying frontal images.

In 1987, a revolutionary advancement in facial recognition occurred with the development of the Eigenface method through the work of Lawrence Sirovich and Michael Kirby. Michael Kirby, a professor of Mathematics at Brown University, worked alongside his colleague, Lawrence Sirovich, a computer science professor at Brown

[26] "Face Recognition." *Or Face Detection Technology*, n.p., n.d.,, http://www.engineersgarage.com/articles/face-recognition?page=2.

[27] A. J. GoldStein, L. D Harmon, and A. B Lesk, "Identification of Human Faces," Proc IEEE, May 1971, vol. 59, no. 5, 748–760.

University, is developing a principal component analysis system or PCA.[28] Their system essentially simplified the numerical values needed to break down the image of the face.

In 1991, Matt Turk and Alex Pentland expanded on the work that Kirby and Sirovich started with Eigenface. Eigenface focused on the frontal image of the face, while the Turk and Pentland study went beyond this initial stage and gave the impression automotive facial recognition was not just a science fiction thought but was becoming much closer to reality.

Another process method similar to principal component analysis is the linear discriminant analysis or LDA. The LDA method was devised from a 1936 R. A. Fisher study on pattern analysis.[29] LDA was similar to PCA and has been the subject of several comparative analysis studies as to which one better performs. LDA and PCA methods are still effective at comparative analysis of images but do not consider other environment factors in the image such as lighting. An additional issue not addressed in these two methods is facial movement.

Elastic Bunch Graph Matching, or EBGM, is the procedure that can distinguish movements in the face. It considers the nonlinear characteristics of face. These are the most common forms of procedures that have been applied to support the development of facial recognition. The development did not transpire without government support.

In 1993, facial recognition technology, or more commonly known as FERET, was established. The program was established to expand on an emerging field of technology and devise an algorithm that will lead to automatic facial recognition. The program was supported by Defense Advanced Research Products Agency and the Department of Defense.[30] It is through this government intervention that the system developed into the structure we have today.

---

[28] L. Sirovich and M. Kirby, "Low-dimensional Procedure for the Characterization of Human Faces," J. Opt. Soc. Am. A **4**, 519–524 (1987).

[29] R. A. Fisher, "The Statistical Utilization of Multiple Measurements, º Annals of Eugenics," vol. 8, 376–386, 1938.

[30] P. Jonathon Phillips, *FERET (Face Recognition Technology) Recognition Algorithm Development and Test Results*, Army Research Laboratory, 1996.

B. TESTING AND IMPLEMENTATION OF FACIAL RECOGNITION TECHNOLOGY.

Even though the initial advanced research into the use of the technology were conducted in the United States, the first public location to implement facial recognition technology in a crime fighting capacity were in Newham, England. In 1997, the United States Company Visionics installed the technology on Cameras in Newham. Newham is a borough of the Metropolitan area of London. Visionics system, known as Faceit, was deployed years later in Tampa Bay, Florida. The Newham project has been deemed a success in crime reduction but it was considered a success more for closed circuit television deployment than facial recognition. In August 2001, data available on the Newham project revealed that 527,000 faces were detected, but only 90 matches of individuals in the database were found. It was still considered a success at the time.[31] Visionics had found the perfect market to advance their system; it was a borough situated about five miles from the City of London with an extensive video surveillance system already in place. In Newham, Visionics found a municipality that was receptive to using this emerging technology as a tool to combat both crime and terror. Around the same time as the borough of Newham experimented with using this emerging technology, casinos and private sector companies had also sought to increase their security with biometrics.

Facial recognition technology continued advancing research though private public ventures until 1999. After the FERET program expired, the National Institute of Standards and Technology sponsored the Facial Recognition Vendors Test or FRVT. This was an organization that evaluated and monitored the progression of the facial recognition development.[32] It is during the FRVT program that perhaps the most noteworthy experiment of the technology takes place within the United States. The fear of a terrorist attack at a major sporting event, such as the Super Bowl, had entered all security planners' mind since the 1972 Munich game attacks that brought terrorism into

---

[31] General Accounting Office, *Technology Assessment Using Biometrics at the Border***,** 175.

[32] Phillips, P. Jonathon, "*Face Vendor Recognition Test,"* National Institute of Standards and Technology, n.d., http://www.nist.gov/itl/iad/ig/frvt-home.cfm.

everyone's living room. The 2001 Super Bowl in Tampa Bay, Florida saw the implementation of facial recognition in order to prevent wanted persons and known terrorists from attending the event. Although a known terrorist, or wanted individual, was not arrested or detained as a result of the technology. The technologies deployment was deemed a success primarily because no major incident occurred. There are a few capabilities that would definitely create a safer society. The ability to identify a known terrorist or criminal whose photograph is in the database as part of a watch list or criminal public record. Yes, if this known individual conducted surveillance on or around a soft target facial recognition, it would likely identify them. There is an additional biometric technology that would be required, gait recognition.

C. HISTORICAL GENESIS OF GAIT RECOGNITION

Gait recognition, a form of biometric behavioral technology would be utilized to detect suspicious behavior. Gait addresses the factors that facial recognition has been plagued by in development. The angle of the subject, lighting of the environment and any disguises by the subject used to elude the technology will be brought out in gait recognition. Gait was developed during the same time period as of biometric technologies. Gait has been studied since the time of Aristotle.[33] There has always been an interest by scientists to analyze why both humans and animals move in a certain way. In the biometric technology, gait systems have emerged as the new process for identifying individuals at a distance. The three algorithms that scientists used to advance this method into a biometric method of analysis are Invariant recognition, Hidden Markov and Shape dynamic method, a three-dimensional method. The algorithms focus more on the three and two-dimensional aspect of the subject recognition. These three algorithms provided the method for future gait recognition research.

If Woodrow Bledsoe, Helen Chan Wolf and Charles Bisson were considered pioneers in the field of facial recognition, then Dr. James Cutting, a psychology professor

33"The Internet Classics Archive, On the Gait of Animals by Aristotle, "The Internet Classics Archive On the Gait of Animals by Aristotle," Trans. A. S. L. Farquharson. M.I.T., n.d., http://classics.mit.edu/Aristotle/gait_anim.html.

from Cornell University, and Dr. Lynn Kozlowski, a psychology professor from Wesleyan University, would be considered the pioneers of gait recognition.

The Cutting and Kozlowski study was conducted in 1977 at the Wesleyan University campus. The Cutting and Kozlowski experiment attempted to determine whether or not students could be identified by the way they walk. The study pointed out that participants recognized individuals by the "bounciness, rhythm of the walker and amount of arm swing of the walker.[34]" Although their study was not focused on the biometric process, it would be the prototype that future scientists would devise for gait algorithm. It contained the factors that were considered synonymous with a specific person. Niyogi and Adelson would be the future scientists who in 1994 led the initial effort in applying the process of gait recognition to an algorithm that would be identified in a computer formula.[35] gait recognition evolved like other biometrics at the time.

Amile Kale, Roy Chowdhury and Rama Chellappa conducted a recognized study into the Invariant recognition algorithm. Their 2004 study was conducted at the University of Maryland. Kale, Chowdhury and Chellappa determined that the best approach to identifying a person from gait recognition is through having the camera parallel to the subject walking. Although the study showed that gait recognition was possible, it was not all encompassing because it recognized that cameras running parallel were not feasible for most surveillance methods.[36] The motion of the subject was important aspect of the detection, as opposed to the model-based detection proposed in the Hidden Markov Method.

The Hidden Markov Method or HMM method relied on the algorithm detecting patterns similar to the anticipated pattern. An example of how best to explain the method can be deducted from something as simple as forecasting weather just based on previous weather. If weather for the last couple of days is rain and snow, then it will continue to be

---

[34] J. E. Cutting and L. T. Kozlowski, Recognizing Friends by Their Walk: Gait Perception Without Familiarity Cues, *Bulletin of Psychonomic Society,* 1977, 353–356.

[35] S. A. Niyogi and E. H. Adelson, Analyzing Gait with Spatiotemporal Surfaces. In Proc. of IEEE Workshop on Non-Rigid Motion, 24–29, 1994.

[36] A. Chowdhury Kale, R. Chellappa, Towards a View Invariant Gait Recognition Algorithm, University of Maryland, 2004, 1–8.

rain and snow. This method does not allow for all potential variables, but it does allow for a simple formula to identify what can be anticipated. If furtive movement is something that can be anticipated in either terrorist or criminals before they act, then the Hidden Markov Method may play a role in gait recognition. Dr. Amile Kale, considered a scholar in gait recognition, also authored an additional study on utilizing the Hidden Markov Method in gait recognition.[37] The method ranks images and allows the process to work on larger databases than most methods. There is no simple process to adequately describe the effort that researchers have shown over the last two decades. It is possible today to identify individuals from their facial features, just as it is possible to identify through the pace or the manner in which they walk.

In a similar manner as facial recognition, gait recognition evolved through the scientific efforts of numerous researchers applying known algorithms in an effort to create an ability to identify individuals through viewing their images.

Figure 2 simply describes how all of this technology will work. The image is grabbed from a closed circuit television camera. Whether the image is stored for gait or facial recognition, it will be broken down utilizing the mathematical equations that will measure the distances between specific points on the image. The images will be compared to pictures stored in a database and results will be sent to a human operator for analysis and dissemination as appropriate.

[37] A. Kale, A. N. Rajagopalan, N. Cuntoor, V. Kruger, University of Maryland, 2002, *Gait-based Recognition of Humans Using Continuous HMMs*.

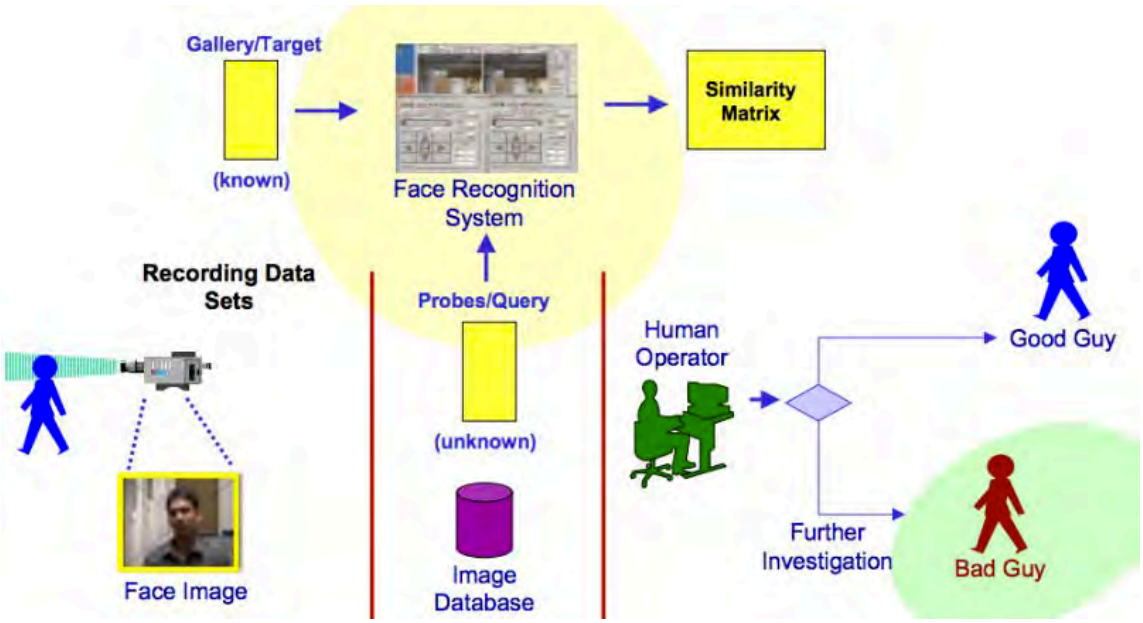

Figure 2. FRVT 2002 evaluation: How recognition technology works[38]

Figure 2 displays how vital the closed circuit television system is to the technology integration process. The technologies, if properly applied, can enhance security for a society that has become apprehensive of about protection. These emerging technologies cannot standalone. Closed circuit television is an essential part of any system that will employ these emerging technologies. Now that these emerging technologies have been explored, the subsequent chapter will look at the closed circuit television systems the technologies will inevitably be deployed with in order to augment security.

This chapter has shown how biometrics, although scientifically complex, can enhance safety and security in society. Closed circuit television systems are a necessary part of this security process and will be discussed further in the subsequent chapter.

38 Jonathon P. Phillips, Patrick Grother, Ross Micheals, Duane M. Blackburn, Elham Tabassi, and Mike Bone, "Face Recognition Vendor Test 2002," In *Analysis and Modeling of Faces and Gestures, 2003, AMFG 2003. IEEE International Workshop on*, 44. IEEE, 2003, http://www.biometrics.org/bc2002/Phillips.pdf.

THIS PAGE INTENTIONALLY LEFT BLANK

III. EVOLUTION OF CCTV, DATA PROTECTION AND PUBLIC PERCEPTION

Closed circuit television is the platform that an emerging technology will need to use in order to facilitate a system that will mitigate the vulnerability of soft targets. The previous chapter looked at the emerging technology, but this chapter will review the closed circuit systems because this will be the foundation for the solution to the problem. The chapter will give a historical perspective, as well as an understanding of the closed circuit system, while explaining how it evolved and worked. The evaluation will look at where the system is utilized, particularly the usage in Great Britain and the United States. The chapter will consider the importance of data protection, as well as view the important ramifications that can develop through the public's perception of a surveillance system.

Closed circuit television, in its simplest form, is the distribution of a video signal in a secured system. Closed circuit television is often juxtaposed with what is commonly known as broadcast television, which transmits an open signal. The progression of monitoring systems has rapidly advanced over the past fifty years. Closed circuit television has been used as a tool in security protection for decades, but it did not begin as a security tool. Figure 3 depicts how the use of closed circuit television can be utilized by law enforcement today.

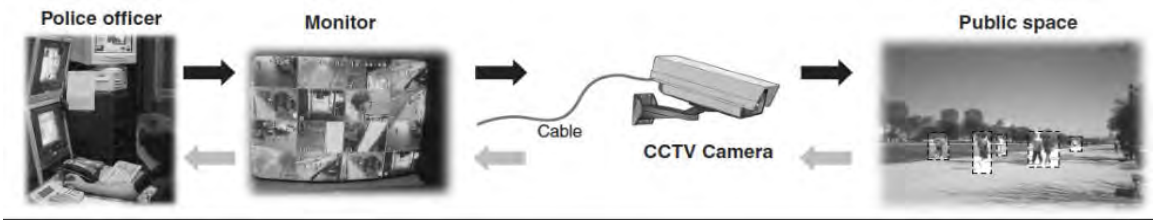

Figure 3. How law enforcement uses CCTV [39]

[39] Video Surveillance Information on Law Enforcement Use, United States General Accounting Office, June 2003.

A German engineer, Walter Bruch, invented the system in order to remotely monitor the launch site of German military rockets.[40] Whether in Germany or the United States, the system was devised as a monitor to assist with the development for other scientific ventures. CCTV has transformed into so much more. Retail stores have used it to detect shoplifters. While casinos have employed the technology to detect fraudulent activity, and banks have developed the technology to identify and prevent robberies, the private and public sectors have successfully embraced the technology to secure their premises.

The initial CCTV systems were analog as opposed to the more modern digital system. The resolution of the image is in essence the primary difference between the two systems, with digital providing a sharper image. Both digital and analog surveillance systems are still in place today. The other significant difference is that the analog system requires the camera to be wired with coaxial cable, while the digital can use an Internet Protocol Access. The latter allows for more flexibility in camera placement and probably led to the dramatic expansion of the CCTV system in the 1990s. Although analog can still provide an efficient service in the CCTV system, the flexibility and accessibly of digital systems led to significant growth.

Although the scientific and military experience of a German engineer may have initially developed closed circuit television technology, it is quite obvious that the implementation process evolved in Great Britain.

A. EVOLUTION OF CLOSED CIRCUIT TELEVISION IN GREAT BRITAIN

Great Britain has been a global leader in the adoption of CCTV. The country has successfully utilized closed circuit television in providing protection for society through surveillance of public areas. In Great Britain, the surveillance system has been in place for decades and initially was developed in order to combat criminal activity in the transit

40 Forrest Lee, "Someone's Watching You: From Microchips in Your Underwear to Satellites Monitoring Your Every Move, Find Out Who's Tracking You and What You Can Do about It," 2011, Adams Media Corporation, 13.

system.[41] The system has evolved into a tool that can be utilized to combat terrorist activity. In the United Kingdom, the number of actual surveillance cameras monitoring the country vary from estimates of 1.85 to 4.2 million; either figure is far greater than the estimated number of cameras in any of the surveillance systems currently monitoring cities in the United States.[42] A major evolution of the British closed circuit television system occurred with the February 12, 1993, death of a two-year old boy named James Bulger.[43] Bulger's senseless kidnapping and murder by two ten-year old boys was captured on the shopping mall closed circuit television system. The video led to the eventual prosecution of the two boys for the murder of young James Bulger. The Bulger abduction video also clarified the need to monitor video surveillance, if it is to be effective in crime prevention or in a counter terrorism capacity.

Although the use of the technology had been initiated in the transit system to prevent crime, it would be this shopping mall private sector video that would magnify the expansion. The British system was not only increased to prevent heinous crimes such as the Bulger murder, but also Great Britain considered CCTV to combat another serious threat, the Provisional Irish Republican Army. Closed circuit television provided the British government the opportunity to identify suspected Irish Republican Army activity in the pre-attack operational stage[44]. The British became the standard that other systems attempted to duplicate.

The home office oversees the CCTV program of Great Britain. Great Britain's system recognizes that a significant amount of cameras were already in place in the private sector. While the home office provides the oversight, the individual municipalities provide the management of the system. Controls gather both public and private video

---

41 Michael McCahill and Clive Norris, "CCTV in London," *Report Deliverable of UrbanEye Project* (2002).

42 Thomas Reeve, "How Many Cameras in the UK? Only 1.85 Million, Claims ACPO Lead on CCTV," *SecurityNewsDeskcom RSS*. Security Media Publishing LTD, 1 Mar. 2011, http://www.securitynewsdesk.com/2011/03/01/how-many-cctv-cameras-in-the-uk/.

43 Tom Sharatt, "James Bulger 'Battered with Bricks," *The Guardian*, November 2, 1993. http://www.theguardian.com/uk/1993/nov/02/bulger.tomsharratt.

44 Nils Zurawski, "I Know Where You Live!-Aspects of Watching, Surveillance and Social Control in a Conflict Zone," *Surveillance & Society* (2005): 508, http://www.surveillance-and-society.org/ articles 2(4)ni.pdf.

surveillance. Operators are trained on how to identify suspicious behavior, as well as an understanding of who the stakeholders are in the project. Law enforcement and the community are considered active stakeholders. The British system considers security everyone's responsibility. The private business sector, as well as individual persons, can call into the control room with any suspicious behavior that is observed. The control room can then monitor the activity and relay necessary alerts to law enforcement or security services. The initial strategy was to unite the private sector with the public sector in an all-encompassing security system. Laws are in place that document what can be collected and stored. The United Kingdom has leveraged their national crime prevention strategy on video surveillance as a crime preventative measure. Great Britain, who historically dealt with terrorist attacks on the Homeland, had public support regarding acceptance of the system, although the cost was always a concern. The success of integrating a CCTV system will always depend on both private and public support. It is estimated that the British government spent five hundred million pounds of sterling on video surveillance development between 1992 and 2002.[45] The public support of this system was driven from such tragic events as the Provisional Irish Republican Army bombings, but the openness of the system allowing public access help strengthen public support.

In 2005, the home office conducted an assessment of the system. The study consisted of fourteen case studies of areas that had integrated CCTV systems into their security system.[46] The cameras were positioned in various areas, which included urban, residential and other miscellaneous locations, such as hospitals. The report revealed a variety of results. Crime was reduced in some areas, displaced in several and increased in others. The results varied for a number of reasons, primarily because the environment and locations of camera installation differed and was a constant variable in the study. The British system employed mobile cameras in areas deemed to be problematic. These problematic zones were high crime areas in which the mobile cameras provided

[45] Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis, Brandon C. Welsh, David P. Farrington Justice Quarterly vol. 26, iss. 4, 2009.

[46] The Impact of CCTV: Fourteen Case Studies, Martin Gill, Angela Spriggs, Home Office Report 15/05.

additional views. In targeting these zones with both video surveillance and deploying personnel to apprehend identified criminals, the system effectively reduced crime. There were environmental factors, such as improved lighting and clear camera view that may have played a role in the crime reduction. In some cases, police actions coincided with camera monitoring and may have performed a significant factor in crime reduction. The clear element was that CCTV was not the only panacea to resolve the problem.

B. EVOLUTION OF CCTV IN THE UNITED STATES

Closed circuit television was used in a similar fashion in the United States for decades. In New York City, cameras were installed in spring of 1983 in the Transit system but the project was stopped in 1985 and deemed ineffective.[47] When the New York City police chief was questioned as to why the project failed, he suggested the failure was due in part to camera placement. There would appear to be other factors as well since camera placement would seem to be an issue that could be rectified. The primary factor would be the limited impact the new system had on the rising crime rate in the New York City Transit System. The cameras were installed under a federal urban transit administration grant and when the funding stopped so did the interest by municipalities in using the technology. In New York's initial experiment into video surveillance, it appeared that the cameras displaced the crime at a time in the city where the crime rate was on a rapidly escalating increase. The system was viewed as a quick fix, and when it had no impact the program was disbanded.

In order to combat auto theft in New York State in 1990s, then Governor Mario Cuomo signed a new law that required active community participation. The" C.A.T." (Combat Auto Theft) Program, as it was known, allowed police to stop a vehicle that had the appropriate decal affixed to their car. The vehicle could be stopped between the hours of one and five in the morning.[48] The owners consented to the program and a decal was placed in the rear window of the car to allow the officers the ability to identify the

---

47 Deirdre Carmondy, "The Subway Anti-Crime Test Abandoned," *New York Times*, October 4, 1985.

48 "All New York Getting Car-Theft Decal Plan," *New York Times*, 19 Aug. 1990, http://www.nytimes.com/1990/08/19/nyregion/all-new-york-getting-car-theft-decal-plan.html.

participating vehicle. In surveillance systems technology implementation, there will be a similar need for community participation, if successful implementation of the program is possible.

Another important aspect of surveillance systems is the protection of the data that is collected. The Regional Information Sharing System, more commonly known as the RISS, is one potential organization that could be part of a system that may be able to oversee the surveillance protection system. It was established over forty-years ago and is overseen by the United States Department of Justice. The RISS is funded by Congress but managed locally.[49]

Historically, the Regional Information Sharing System is responsible for the protection and sharing of criminal data, with oversight from the United States Department of Justice. Data sharing and protection are a significant aspect of any new surveillance system.

In the United States, the video surveillance systems were under the control of the individual municipalities and developed over public and private partnerships. There were federal grants provided for surveillance closed circuit television systems in transit facilities, but most appeared to be a means of obtaining funding without adequate local support. It took decades to develop the system that Great Britain currently has in place. The British people seem to be more accepting and supportive of a surveillance society. The framework of the British system that provided methods for both the public and private sector to be involved and aware of the surveillance may have created some of the support, but initially, support was drawn from the need to do something to protect the homeland that had seen first hand the impact of terrorist attacks.

The support in the United States would finally arrive when the image of Mohammed Atta walking though a security check point in a Portland, Maine airport on September 11, 2001, and was broadcast throughout the world. The 911 hijackers walked unnoticed through security checkpoints that day and forever changed the way security experts would view surveillance footage.

[49] "Regional Information Sharing Systems (RISS)," 21 Nov. 2013,http://www.riss.net/.

After September 11, 2001, the United States saw a dramatic expansion of the closed circuit surveillance system. An interview of Khalid Sheik Mohammed resulted with the identification of an Indian national named Dhiren Barot. Barot was a person who entered the United States in April 2001 on a student visa, but never attended school, instead spending his time conducting surveillance on targets in New York and Washington. Barot's surveillance project consisted of identified locations where video surveillance existed.[50] Although Barot's plot was detected before it could be carried out, it was just another example of the role closed circuit television played in counter terrorism protection. In August 2004, Barot would be arrested in Great Britain after extensive closed circuit television surveillance of his activity.

Just as Great Britain did not see the closed circuit television as exclusive toward terrorism protection, the United States looked at the crime prevention roles these systems offered as well.

In June of 2003, the United States General Accounting Office produced a report that issued information on law enforcement's use of CCTV. The report gave an overview of how the systems worked, as well as identifying a select group of agencies that were using the technology. One of the interesting points that the report provided was identifying the training issue with most United States' systems. The United Kingdom provided agencies or municipalities training alongside the vendor training, while most United States cities relied strictly on the vendor training and held no additional agency training. Training standards by individual agencies or municipalities may clarify the mission and insure that respective both agency and/or city guidelines are adhered to as well. The four cities mentioned in the government report all had different methods of utilizing their respective systems. Baltimore's system was, for the most part, not monitored. Columbia, South Carolina allowed for remote monitoring in patrol cars. Virginia Beach and Tampa Bay only monitored their systems during high pedestrian traffic times, such as weekends or tourist seasons. New York City has over four thousand

50 Thomas Kean, Lee Hamilton, R. Ben-Veniste, B. Kerrey, F. Fielding, J. Lehman, J. Gorelick, T. Roemer, S. Gorton, and J. Thompson, "National Commission on Terrorist Attacks Upon the United States," *Washington, DC* (2004), https://www.fas.org/irp/offdocs/911comm-sec5.pdf.

cameras throughout the city in their new Domain Awareness System. The training, like most municipalities, is carried out by the vendor and not by the department.

A 2012 study was conducted that analyzed the effectiveness on the Chicago closed circuit surveillance system. The Chicago system consisted of over one thousand cameras in a two hundred square mile radius.[51] The study revealed a reduction of crime in high-crime areas where the cameras were placed. There were also other factors, such as increased law enforcement presence in these areas. As a result, it was not determined whether the increased law enforcement presence or cameras led to the reduction. The analysis also showed that where cameras were monitored, the effectiveness rose. There is one closed circuit television system that has been properly deployed on both sides of the Atlantic, the automated license plate reader system.

C. AUTOMATED LICENSE PLATE READERS

Automated license plate readers are another form of closed circuit television technology that is used to identify traffic flow in numerous municipalities around the world. Automated license plate readers were first used in Great Britain. This technology, like other emerging recognition technology uses an algorithm to identify the license plate that passes the monitor of the system. The system has advanced to the point where the technology has been incorporated into modern traffic technologies, such as red light detection cameras, stop sign cameras and speed monitoring technologies. All of these technologies evolved from the automated plate reader that detects the vehicle, photographs it and identifies it through an additional photograph of the license plate. Although the technology was initially devised to monitor traffic safety and movement, the system has evolved into a surveillance system that can track the location of vehicles. The system has expanded from stationary locations, such as tollbooths to mobile operational equipment placed on police vehicles. The system provides a platform for future emerging technologies, and up until this point, has not shown a negative impact on the public's perception of surveillance regarding their safety.

[51] Rajiv Shah and Jeremy Braithwaite, "Spread too Thin: Analyzing the Effectiveness of Chicago Camera Network on Crime," Police Practice and Research: An International Journal, April 2012.

In the 1970s, Great Britain had experienced numerous Vehicle Bourne Improvised Explosive Device (VBIED) detonations by the Provisional Irish Republican Army. The integration of a system that could track vehicles would play a much greater counter-terrorism role than simply monitoring traffic. Automated Plate Reader technology would lead to identifying the vehicles in the VBIED bombing attempts in London and Glasgow in 2007.[52] The system provides a successful framework for how to integrate future emerging technology systems. The identity, as well as the vehicle location and real time notification to law enforcement on the street, is a similar method that will be used in emerging technologies. There is also the investigative forensic and intelligence gathering capability that a system such as this can provide. The ability to identify vehicles of suspected terrorists or criminals and place them in close proximity to a target or incident is a significant aspect in both a terrorism and criminal investigation. Automated Plate Reader technology has shown that proficiency.

D. ANALYSIS OF BRITISH AND UNITED STATES CCTV SYSTEMS

The initial analysis shows that the British system has shown dramatic success in crime reduction and CCTV implementation. The British system provided oversight on all aspects of the closed circuit system from the outset. The home office provides guidelines for local government. The municipalities are a separate entity in the surveillance system. Although in Great Britain, both law enforcement and the domestic intelligence gathering systems are agencies that have access to the surveillance system, the fact that they are not the primary agency managing the system adds a layer of protection for the public. Civil libertarians in the United States constantly question the police use of surveillance systems. As with British systems in which municipalities run many of the surveillance systems, a separate agency managing the cameras could be the remedy that will provide the critics of surveillance in the United States less impetus in claiming an Orwellian society is being developed.

---

[52] Cara Buckley, "New York Plans Surveillance Veil for Downtown." *New York Times,* 9 July 2007, .http://www.nytimes.com/2007/07/09/nyregion/09ring.html?n=Top%2fReference%2fTimes%20Topics%2fSubjects%2fT%2fTerrorism.

In addition to a separate agency being used for oversight, the Data Protection Act in Great Britain addresses, among other things, the rights and protection of individual liberties. It provided the public assurance that there were procedures in place that would protect individual liberties. In the United States, the individual municipality controlled guidelines and procedures. Often for an individual citizen in the United States to request these respective guidelines from their municipality, if in fact they existed, it would require a Freedom of Information Act request, which could also be time consuming in bureaucratic red tape. The system in Great Britain not only outlined guidelines, procedures and what was actually legal under the Data Protection Act, but a separate code of practice existed by the home office and the individual municipalities that administered the cameras.[53] The structure and oversight in the United Kingdom no doubt plays a significant role in assuaging any public concern.

Another success in Great Britain came from the extensive surveillance system that was already in place. The forging of public and private partnerships in a cooperative effort in devising an all-encompassing security blanket took time to develop. In the United States, with the exception of a few cities, the surveillance systems consisted of a few cameras that are occasionally monitored. In some cases, the personnel monitoring the cameras systems are in limited duty status and specifically trained for closed circuit surveillance system monitoring.

E. DATA PROTECTION

Data Protection, as part of the closed circuit surveillance system, has been a concern in the European Continent since the onset. The individual states, as well as the European Union, have Data Protection laws. The New York City Police Department has developed guidelines concerning data storage and collection.[54] There are many complex

---

53 "Surveillance Camera Code of Practice," Www.gov.uk. June 2013. London: The Stationery Office, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf.

54 New York City Police Department, "New York City Public Security Guidelines." Last modified April 2,
2009. http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/public_security_privacy_guidelines.pdf.

issues that coincide with enhanced surveillance of society. It appears society's acceptance of such a system is first and foremost, but any policy must insure that in society acceptance, the government provides necessary checks and balances to provide protection to their citizens' inalienable rights.

One Norris and McCahill study pointed out how the "effectiveness of the whole system is dependent on the quality of the captured image."[55] Norris and McCahill are correct. The system's success has been driven by the quality of the captured images. The protection and security of these captured images must also be regarded as an important consideration of the system. The British have recognized the importance of quality images and in integrating the technology as well as data protection.

Data Protection is a concern and Great Britain has shown a concern from the outset. There are data protection acts in both Great Britain and the European Union to assure protection of citizens under the CCTV surveillance systems. The London transport system provides information on their website of how an individual customer can obtain copies of personal images that were taken of them on the transport system.[56] In the United States, an individual can petition a governmental agency in what is known as a Freedom of Information Law (FOIL) request of government records, but there is no guarantee that their FOIL request will be immediately released upon request. CCTV systems already recognize a process for data protection. A similar process will need to be put in place on an emerging technology policy.

Clive Norris and Gary Armstrong wrote *Maximum Surveillance Society: The Rise of CCTV*. Norris and Armstrong give both a historical perspective and anthology of the use of video surveillance by law enforcement. Norris and Armstrong focused on the success that the British Government had integrating this technology into law enforcement

---

[55] Surveillance & Society CCTV Special (eds. Norris, McCahill and Wood) 2(2/3): 110–135.

[56] "CCTV, "*Home*," Transport for London, Aug. 2011, http://www.tfl.gov.uk/assets/downloads/businessandpartners/cctv-guidelines-for-taxis-and-phvs.pdf.

practices. Norris and Armstrong did point out "the exponential increase in visual surveillance creates a massive and costly problem of information processing and handling." [57]

Data protection and privacy protection are two primary issues concerning the implementation of surveillance technology. In Europe, the data protection and privacy laws have evolved over the years as the technology has grown. A recent New York Times article compared and discussed data protection laws within Europe and the United States. The European Unions "blanket regulations" juxtaposed to the United States system of allowing industry specific regulation or self-regulation. [58] The European Union is currently devising new data protection reform that will regulate the data collected in all European Union States. In Europe, the protection policy is predisposed toward the individual rights to access the data collected on them. In the United States, the individual can access the data collected but generally will require a court issued subpoena. The United States system appears to put obstacles in the way of the access. The United States system does allow for greater control of the data but in doing so may infringe on individual liberties. The individual liberties are protected under the Fourth Amendment of the United States Constitution.

F. PUBLIC PERCEPTION OF SURVEILLANCE

Although a recent Quinnipiac College poll of New York City voters found that 82 percent of New York City voters supported the increased use of surveillance cameras in public space, [59] public acceptance is not the only concern. The video surveillance of individuals in a public street, who are not the subject of a criminal investigation, may be a concern to these individuals.

---

57 Gary Armstrong and Clive Norris, "Maximum Surveillance Society: The Rise of CCTV," Sheffield University, 1999, 210.

58 Nathsha Singer, "Data Protection Laws, an Ocean Apart," *New York Times*. 2 Feb. 2013, http://www.nytimes.com/2013/02/03/technology/consumer-data-protection-laws-an-ocean-apart.html.

59 Maurice Carroll, ed., *New York City Voters Smile for the Security Cameras, Quinnipiac University Poll,*, [Quinnipiac University, 23 May 2013], http://www.quinnipiac.edu/institutes-and-centers/polling-institute/new-york-city/release-detail?ReleaseID=1897.

There is an increase in acceptance of surveillance by New Yorkers, but it should be pointed out the survey was taken after the Boston Marathon Bombing. In New York, it is a public private partnership controlled by the police department. In other parts of the United States, the system is self-regulated. The Department of Homeland Security provided monies to install surveillance systems, but the operational guidelines appear to have been under the control of the individual municipalities. The United States Justice Department provides guidelines, but the individual municipality controls the system. The greatest concern the public may have been in any self-regulated system is insuring the data gathered is protected.

This chapter reviewed the technology of closed circuit television, the data protection legislation in the United Kingdom and the significant role it plays in surveillance systems. The section also looked at the public perception and the important role that perception can play in a surveillance system. The chapter gave an historical perspective, as well as a discussion of how the technology is currently being used as a security protection instrument and showed where the system encountered success and disappointment. The subsequent chapter will look at the privacy and legal concerns with employing this technology that will need to be addressed in order to actively apply this technology in an emerging system. Ultimately, the foundation of these systems will lead to how future systems will succeed or fail.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. EXAMINE LEGAL AND PRIVACY ISSUES WITH EMERGING TECHNOLOGY

Any system that mitigates soft target vulnerability through utilization of closed circuit television and emerging technologies will require very structured guidelines to insure that individual liberties are not impeded throughout the process. Previous chapters have shown the technology, and how it has been implemented in the past. Case studies have been analyzed to develop a framework of how the future process should be applied. The predominant concern in any free society is individual liberty. The debate of any surveillance system will always need to create a balance between individual liberty and security. The video surveillance of individuals in a public street, who are not the subject of a criminal investigation, may be a concern to many persons in a free society. When initially delving into the principle of whether it is right or wrong to conduct surveillance activity in a free society, the preliminary interpretation would be the belief that a search warrant from a judge must be necessary to conduct such an operation. In order to better understand the process, it is best to look at how courts have addressed this issue.

A. FOURTH AMENDMENT-SEARCH AND SEIZURE

In the United States, the Supreme Court would bear the ultimate burden on whether law allows for such intrusion on individual liberty. The two primary Supreme Court decisions that guided the law enforcement utilization of the technology are Katz vs. United States and Kyllo vs. United States. In both cases, the court ruled that the Fourth Amendment right did not extend to a public area. It should be noted that there is no specific case law directed at the issue, but the court rulings were based on previous electronic surveillance.

On the June 11, 2001, Kyllo ruling, the court cited that "just as an individual does not have a right to an aroma that leaves their kitchen and goes outside so to they do not have a right to thermal heat leaving a premise." [60] The Kyllo case involved law

[60] Kyllo vs. United States 533 U.S. 27 (2001), http://laws.findlaw.com/us/533/27.html.

enforcement utilizing thermal detection equipment to determine if lighting conducive to marijuana growth lamps existed inside a location.

The Katz case involved law enforcement monitoring a listening device on a public payphone. On December 18, 1967, the Supreme Court ruling stated, "What a person knowingly exposes to the public they do not have a right to privacy on." [61] Of course, neither of these cases involved the technology currently under review, but the courts have shown a propensity to support law enforcement's use of technology in a public place. Even though it would appear that the policy would be in compliance with Fourth Amendment concerns, the perception by those opposed and the political ramifications of opposition must also be considered in any implementation.

An additional case that would support an individual's reasonable expectation of privacy is found in California vs. Greenwood. The case involved police gathering evidence from garbage that Mr. Greenwood had discarded from his house and set aside on his curb for garbage pickup. Mr. Greenwood's attorney appealed his client's conviction citing the initial confiscation of evidence that was picked up from his garbage can was a warrantless search. The court ruled that an individual does not have a reasonable expectation of privacy on something he or she discards. The ruling was a clear indication of where the court stood on an individual's reasonable expectation of privacy in a public place.[62]

The final Supreme Court ruling that explained why it is necessary that a procedure is needed to be a foundation for closed circuit television operators who will be operating the emerging technology system is Terry vs. Ohio. In Terry vs. Ohio, the ruling was supportive of law enforcement's ability to stop an individual for reasonable suspicion.

On October 7, 1963, a Cleveland police officer stopped John Terry, frisked him and recovered a firearm. The defendant's attorney claimed that his Fourth Amendment right was violated. The case eventually came before the Supreme Court and on June 10,

---

61 Katz vs. United States 389 U.S. 347 (1967), http://laws.findlaw.com/us/389/347.html.

62 California vs. Greenwood 486 U.S. 35, http://laws.findlaw.com/us/486/35.html.

1968, the court ruled that the officer could stop and frisk an individual who he reasonably suspects is committing, committed or is about to commit a crime. The court allowed, in that stop, the officer's ability to frisk, if he or she reasonably believes the individual stopped presents a danger or is armed. The significance in this ruling is that court went on to explain that the reasonable suspicion could not just be a hunch, it had to be an articulable reason explaining the totality of the circumstance around the stop. Any implementation of a surveillance system should consider the Terry vs. Ohio ruling and insure that operators of a system are trained in what would be considered a justified and constitutional stop.[63]

The operators cannot just be spectators viewing a monitor, but they must have a clear understanding of what may be considered a preliminary, criminal or terrorist activity. The operators of the system must also understand the importance and the parameters of the case law that guides the surveillance system. The adherence to a policy that protects the constitutional rights of both those who are under surveillance and who are conducting surveillance is important.

In the New York City Police Department surveillance of political groups led to the Handschu court ruling that set a policy in place. This policy governs the way surveillance procedures can be conducted in criminal investigations of political groups in New York City. The Handschu guidelines were derived from a 1971 court case in which an appellate court ruled in that the New York City Police Department improperly conducted surveillance and in doing so violated a political group's First Amendment right to free speech.[64] In essence, the court ruling sets guidelines for the New York City Police Department to follow when investigating political activists involved in suspected criminal activity. A Handschu committee was established to review any criminal investigations of political activist organizations. Any system that is put in place should anticipate a preconceived perception of the police overstepping their boundaries in conducting surveillance activity.

---

63 Terry vs. Ohio 392 U.S. 1. http://laws.findlaw.com/us/392/1.html.

64 HANDSCHU vs. Special Services Division 288 F.Supp.2d 411, http://www.nyclu.org/files/8.6.03_Handschu_Guidelines.pdf.

By insuring all legal concerns are in a transparent procedure should limit both the political and media concerns that may arise with implementing an emerging technology system.

B. POLITICAL

When looking at what political ramifications may arise in utilizing emerging technology in soft target protection, the first challenge must be to understand who the stakeholders are in the process. It is understood through case law, that an individual does not share the same right to privacy that he or she would have in his or her own house. The limitation on one's privacy does not eliminate the expectation of safety and security that they may presume exists in that same public place. The community and the municipality are the primary stakeholders in this security process.

Of course any product vendor will assure a municipality that his or her product is the finest on the market. The municipality must consider the ramifications on all the stakeholders in the community. If the goal is to prevent crime and reduce the risk of terrorists' attacks, then the stakeholder will be any individual who is impacted by the ineffectiveness of this goal being realized. Historically, in the United States, the American Civil Liberties Union has been the nonprofit organization that has moved forward to insure that the individual's liberties and rights are not discarded in an effort by government to obtain the goals of the stakeholders.

When reviewing studies about closed circuit television and facial recognition, the primary critic of these projects has been the American Civil Liberties Union, also known as the ACLU. In a report that was issued in 2006," *Who's Watching? Video Camera Surveillance in New York City and the Need for Public Oversight,"* the ACLU criticized the surveillance system in New York City. The focus of the criticism was the concern of public notice, storage of data and training of personnel involved in the project. The American Civil Liberties Union was engaged in similar processes in both Tampa Bay and Virginia Beach, where previous facial recognition projects were implemented.

In Tampa Bay, the ACLU submitted a Freedom of Information Act Request for any logs maintained by the Tampa Bay police that listed individuals who triggered alerts

in the facial recognition system. The logs showed limited documentation about the activity. Although Tampa Bay had a policy in place, which included a logbook, there was no oversight that insured the reports were properly maintained. Through political pressure, the ACLU requested this information oversight, which should have been instituted from the start. It would not seem unreasonable to expect maintenance of records in such an innovative project. It should have been a part of any policy of surveillance that was implemented. The maintenance of records and assurance that there is supervision over these records can ease some of the tension between the municipality and political action groups that may be initially diametrically opposed to the process.

It is also difficult to argue with some of the ACLU requests that were recommended in the New York report. Public notice, storage of data and training of personnel should be a part of any surveillance system. It would appear that building a policy that consisted of guidelines that allowed for transparency would not be overreaching.

There was a request by the ACLU for penalties for those individuals who violated the code of conduct that was put in place for operators of the system. There are penalties for misconduct in many agencies, but the key factor is preventing the misconduct, which can sometimes be a daunting task. An audit or self-inspection process in which supervisors review the activity of the operators is also an evaluation process that can be implemented for employees. Crime and the fear of future crime have driven the reasoning behind the need of surveillance systems in today's society. The opposition to the fear driven paradigm suggested that there were inconsistent studies that would find a direct correlation between video surveillance and crime reduction.

The British studies would tend to support the strategy that video surveillance can reduce the crime rate. Campbell Collaboration produced the most comprehensive study that supported closed circuit television effectiveness on crime.[65] The study reviewed forty-four individual case studies on the impact of closed circuit television systems. One of the studies important findings was to recognize the need for independent evaluation of

[65] B. P Welsh and D. C. Farrington, "Effects of Closed Circuit Television Surveillance on Crime," Campbell Systematic Reviews 2008:17.

the system. The study looked at crime conditions before and after systems were implemented and covered cities, town centers, public housing, transportation facilities and car parking areas.

The experience in the United States has not yet produced the same results and allowed for a diametrically opposed political argument, which brings the argument of fear regarding a rise in crime against the creation of an Orwellian society. In order to win the political argument to enhance surveillance, there will be a need to create similar procedures, codes and policies that will generate the trust among the various stakeholders in this project. The media will need to be employed to make sure the messages are explained to the stakeholders.

C. MEDIA

An April 30, 2013, CNN poll revealed that eighty-one percent of the American's surveyed said they supported an expansion on video surveillance. An additional seventy-nine percent stated that they would support the use facial recognition to scan for terrorists at various locations and public events.[66] The polls are a possible indication of political climate change, as well as a possible acceptance by Americans of emerging technologies to combat terrorism. The CNN poll was taken two weeks after the Boston Marathon bombing and showed the influence that this tragic event had on the political climate in the United States. It also is an example of how the media can be employed to assess the public's perception of a technology that is emerging. The belief that it will make the public safer superseded any concern that the individuals had about the government intervening in their lives. The media can play a role in the ability to either undermine or implement the emerging surveillance process.

In Ybor City, US News and World Report wrote about an article profiling the facial recognition. The article showed an image taken from CCTV footage of Robert Milliron but did not mention anything specifically about him. A woman in Oklahoma would wrongfully identify Mr. Milliron as her ex-husband, who was wanted on a warrant.

66 CNN.COM, 1 May 2013, CNN|TIME|ORCPOLL5, http://i2.cdn.turner.com/cnn/2013/images/05/01/top5.pdf.

Officers then used the image to identify Mr. Milliron and visited him at a construction site were he was working. Upon further investigation, the officers realized Mr. Milliron was not the man that the woman in Oklahoma identified.[67] In the media, critics of the technology reported this as a failure of facial recognition. In actuality, the image was taken for the story, but Mr. Milliron was not identified as a perpetrator of any crime in the article. The false alert was not due to technology failure but to a confused individual in Oklahoma. Although Mr. Milliron felt he was treated like a criminal, he was not arrested. The case is an example of how important the media's influence can be and how important it is to get the real story out to the public. It is precisely because of incidents such as this that policy makers must be cognizant of the influence the media can have with a project and insure that the correct message is relayed and brought to the public's attention. The media can present that necessary message of transparency, but they can also derail a project if policy makers do not realize the role they will play in integration.

D. CONCLUSION

The primary reason for graduate research on this topic is to expand on a CCTV system that is currently in place and devise a system that will be the foundation for the future of law enforcement by integrating emerging technology. The technology provides a nonintrusive method with the ability to scan millions of faces in a public place in seconds. There is no amount of personnel that could physically participate in such a project. The technology increases law enforcement's ability to conduct surveillance in public areas and should greatly improve security. It will allow the opportunity to identify individuals before they can act.

This chapter has clarified the legal, privacy, media and political concerns that may develop in putting a system of this nature in place. The next chapter will evaluate how CCTV, combined with emerging biometric technologies, were used in the past and devise an outline of how this past use will lead to future integration.

---

[67] David Avexander and Jacob Richert-Boe, "Ethica of Facial Recognition," 2002.

THIS PAGE INTENTIONALLY LEFT BLANK

V. EVALUATION OF PRIOR PROJECTS–CASE STUDY

The thesis has shown both the technology and the platform to revise it. The focus will now be on how the technology has been applied in the past. In order to develop best practices/lessons-learned for a model for integrating facial recognition into CCTV systems in the future. The past application will be analyzed in order to develop a constructive method to utilize the technology in the future. The data sources consisted of reports about CCTV utilization in several jurisdictions.

The case study analysis will be the method used to identify a solution. Facial recognition technology was implemented with CCTV surveillance systems in the 2001 Super Bowl, Ybor City, Florida, Virginia Beach and at Newham, England. There are many lessons that can be learned from the selection of these case studies. In selecting these case studies, the research has focused on identifying how these studies focused on legal and privacy concerns and whether or not these municipalities saw these emerging technologies as effective at deterring and investigations of crimes. These case studies will also be viewed from the perspective of how did these municipalities integrated the technology approach and deployed the CCTV cameras.

A case study review of these projects successes and failures will be conducted in order create a more effective, viable system for integrating facial recognition technologies into CCTV systems. Concern over accuracy of identification and the privacy, legal and political ramifications regarding privacy are steps that can be applied to each of these venues in order to judge the success or failure of their programs. The accuracy of the identification will be examined to determine best practices in response to false alerts or exact identifications. Privacy will be scrutinized to consider the factors that were used to define privacy concerns of those under surveillance. The legal and political will outline the environment in which this technology was applied.

Success could be defined with crime reduction and one hundred percent identification of wanted criminals or terrorists, but there is no easy measure for success or failure because the parameters are more difficult to define. If the known criminals or

terrorists avoided these areas of surveillance because there was public knowledge of the system in place, it is one factor that is not easily definable. In most cases of emerging technology, the system is never one hundred percent accurate, which is why it is important that the steps that have been chosen in evaluating the framework and procedures that are in place measure success. Organizations must utilizing the technology in a manner that documents the use and provide a mechanism for the privacy, legal and political concerns to be addressed. The types of individuals stopped and whether or not they pose a threat will determine the measurement of success.

In addition to the above criteria, determination will be made of what other factors can contribute to the project's success or failure. One factor to analyze is the camera location and whether or not the locations have an impact on the results of the project. The finding will be used to gain an independent understanding of the technology integration. In the first case study, false alerts were not an issue because the environment was controlled entering the venue.

A. FIRST CASE STUDY–SUPER BOWL XXV IN TAMPA BAY, FLORIDA

1. Background

Super Bowl XXXV was held in January 28, 2001 in Tampa Bay, Florida. Any event of this magnitude is always a concern to security planners. Although the event was held prior to September 11, 2001, the concern of a terrorist attack at major sporting event, such as the Super Bowl, had been fear of security planners ever since the 1972 Munich Olympic tragedy. In Munich, the terrorist group Black September entered the Israeli National team's Olympic Village apartment, took members of the Israeli team captive and ultimately held the world hostage. Their actions led to the death of these Israeli athletes. In the years subsequent to the Munich attacks, American novelists Thomas Harris and Thomas Clancy would both author books chronicling acts of terror involving Palestine terrorist groups at the Super Bowls.[68] Although only novels the thought of a similar act would rekindle fear for a new generation.

[68] Steve Coll, "The Super Bowl's Journalism Malfunction," *The New Yorker*. Conde Nast, 5 Feb. 2013, 24 Nov. 2013, http://www.newyorker.com/online/blogs/comment/2013/02/super-bowl-blackout.html.

The company Viisage Technology was the Massachusetts based business that supplied the software used by the Tampa Bay Police Department.[69] The project consisted of thirty-two cameras deployed at all entrances of Raymond James Stadium.

2. Findings

The database collected images, which consisted of 1700 known criminals. It is important to note that the database contained known criminals and not necessarily wanted individuals, although Eric Robert Rudolph, the fugitive from the 1996 Olympic bombing, was a photo contained in the database.

The hundred thousand fans that entered the stadium were scanned as they approached the turnstiles. The findings revealed that nineteen individuals had prior criminal histories, but no arrests were made as a result of operating the technology. The study alleged one hundred percent accuracy. Perhaps the socioeconomic factor, such as the three hundred twenty dollar minimum ticket price, may have played role in the low number of criminals identified at the event. The fans entering the venue were not aware that their images were being scanned through a database of known criminals. The event drew much media criticism days after the occurrence when it was revealed that this emerging biometric technology was used on fans entering the stadium. A February 2001 Time Magazine article called the event the "Snooper Bowl,"[70] but supporters of the technology saw this test as a success.

B. SECOND CASE STUDY–YBOR CITY, FLORIDA

1. Background

In 1886, Vicente Martinez Ybor moved his cigar factory from Key West, Florida to a track of land approximately two miles east of the city of Tampa Bay, Florida.[71] At the time, Mr. Ybor would have been considered what one would call today a disruptive

---

[69] Lisa Greene, "Face Scans Match Few Suspects." *http://www.sptimes.com*. Tampa Bay Times, 16 Feb. 2001, Web, http://www.sptimes.com/News/021601/TampaBay/Face_scans_match_few_.shtml.

[70] Lev Grossman, "Welcome to the Snooper Bowl," *TIME.com*. Time Inc., 12 Feb. 2001, Web. 24 Nov. 2013, http://content.time.com/time/magazine/article/0,9171,999210,00.html.

[71] "Ybor Story," *Welcome to Ybor City*. Ybor City Chamber of Commerce, 2011, Web. 24 Nov. 2013, http://www.ybor.org/ybor-story.

innovator. He left Key West, Florida due to an inability to attract a labor force. He found in what would be later known as Ybor City, a location that had easy access to Tampa Bay's ports and rail transportation, as well as a thriving immigrant labor force, to work in his factory. At one time, Ybor City was home to the leading cigar producers in the world, but as the cigar production industry faded the community fell on difficult economic times.

Ybor City's revival occurred in the 1990s with urban developers utilizing the old architecture to create a thriving economic entertainment neighborhood. In an effort to enhance security in what was becoming the City of Tampa Bay's center for nightlife, the Tampa Bay Police Department signed an agreement with Visionics Faceit technology. Visionics, a New Jersey based corporation, offered the technology for free as a test project. This was a savings of thirty thousand dollars, which is the usual investment cost of the technology.

2. Findings

Tampa Bay had invested forty-five million dollars in revitalizing the area, so they eagerly accommodated Visionics' offer.[72] On August 2, 2001, the Tampa Bay City Council approved the use of the surveillance system supplied by Visionics.[73] The technology consisted of a database of runaway teenagers and wanted persons. There are thirty-six cameras located on Seventeenth Street, which is the highest pedestrian traffic section in the area.[74] It is estimated that the Ybor City area has an inflow of approximately 125,000 people on a Friday night.[75] Ybor City was the first municipality in the United States to install such a system. The Ybor system was coordinated from a control room a block away from the camera location. An officer monitored the cameras

---

[72] Tampa Police Department Installs Visionics' FaceIt Technology in Anti-crime CCTV Initiative - L-1 Identity Solutions." *Tampa Police Department Installs Visionics' FaceIt Technology in Anti-crime CCTV Initiative - L-1 Identity Solutions*. Visionics Corporation, 29 June 2001, Web, 24 Nov. 2013, http://ir.l1id.com/releasedetail.cfm?ReleaseID=208637.

[73] Amy Herdy, "Civil Rights or Just Sour Grapes?" *http://www.sptimes.com/,* Tampa Bay Times, 3 Aug. 2001, Web, http://www.sptimes.com/News/080301/TampaBay/Civil_rights_or_just_.shtml.

[74] Lane DeGregory, "Click. BEEP! Face Captured," *Tampa Bay Times*, 19 July 2001, http://www.sptimes.com/News/071901/Floridian/Click_BEEP_Face_captu.shtml.

[75] Ibid.

and selected individuals on the camera's view and entered these individuals' images into the database for a comparison against known runaways and wanted individuals. The facial recognition project was discontinued two years after it started with no individuals arrested as a direct result of the technology's use. The Tampa Bay Police Department noted that they were unable to determine how many wanted individuals avoided the area because of the public knowledge that the system existed.

The Ybor City project received criticism from the outset. The America Civil Liberties Union, as well as the media, focused on the privacy concerns. There were protests in the Ybor City area on a weekly basis. The major failure would appear to be leveraging the technology's success or failure on whomever the officer was monitoring the computer screen in the operation room. There did not appear to be any specific parameters in which the officer selected to check against the database. It appeared that the officer's experience in identifying suspicious behavior in a crowd was part of the process on how he or she decided to identify an individual image to check in the database.

C. THIRD CASE STUDY–VIRGINIA BEACH, VIRGINIA

1. Background

On Tuesday November 13, 2001, the Virginia Beach City Council voted 9-1 to install facial recognition cameras in the high-pedestrian traffic area of Atlantic Avenue in the resort area.[76] There were a number of factors that led community leaders to this decision. The two primary factors were the concern over privacy and the influence the September 11, 2001, attacks had on the community. The decision was made two months after September 11, 2001, attacks, so the need for enhancing security by any means was a priority across the county. Virginia Beach, a seaside resort area had historically relied on tourism as an essential part of their economy. The successful use of the technology at the 2001 Super Bowl opened the eyes of many municipalities around the country who looked for enhanced security measures. The 911 Commission would later reveal that an FBI

76 Jabeen Bhatti, "Resort City Approves Using Face-recognition Technology," *The Washington Times*, 15 Nov. 15, 2001, http://www.washingtontimes.com/news/2001/nov/15/20011115–031140–1892r/.

investigation into the attack contained surveillance footage from a bank in Virginia Beach where it was alleged that Mohammad Atta cashed a check in April 2001.[77] The software, Faceit by Visionics, was the same system installed in Ybor City, Florida. Visionics charged the City of Virginia Beach 200,000 dollars, but 150,000 dollars was covered by a grant from the state of Virginia.

2. Findings

The Virginia Beach project consisted of a database of 2,500 wanted individuals. The surveillance system consisted of eighteen cameras located in the Atlantic Avenue area from Seventeenth Street to Twenty-fifth Street. In a similar method to the Ybor city project, officers monitored the surveillance system and when alerts were detected, the computer monitoring officer or CMO would notify the supervisor and responding officer as dictated by the type of alert. The Virginia Beach Police Department established a strict set of guidelines and protocol for officers who were monitoring the video system to follow.

There were number of challenges with the facial recognition product. During the time of installation, Virginia Beach did not affect one arrest as a result of the technology. There were technical challenges with the software that produced false alerts. The vendor who the city initially purchased the software from merged with a new biometric company, Identix, which did not fully support the initial product that Virginia Beach purchased. In October 2005, the program was discontinued.

The Virginia Beach project appeared to be the case of a vendor advising the municipality about what they really needed as opposed to the municipality telling the vendor this is what is actually needed. It also appeared that the municipality lost interest in making the product work once the grant funding had subsided.

---

[77] Thomas Kean, Lee Hamilton, R. Ben-Veniste, B. Kerrey, F. Fielding, J. Lehman, J. Gorelick, T. Roemer, S. Gorton, and J. Thompson, "National Commission on Terrorist Attacks Upon the United States," http://govinfo.library.unt.edu/911/report/911Report_Ch7.htm.

D. FOURTH CASE STUDY–NEWHAM, ENGLAND

1. Background

Newham, England, located in metropolitan East London, has a population of two hundred fifty thousand people. In 1997, Visionics offered their facial recognition technology in an effort to reduce crime in Newham. Newham already had an extensive closed circuit television system in place. The surveillance system was operated by the Newham Security Department, which was separate from the Metropolitan Police Service. Unlike the facial recognition projects in the United States, the Newham Council received ninety-three percent approval rating for the project from the residents.[78]

2. Findings

The public support and extensive surveillance system already in place are two of the primary factors that led to the Newham project's success. Newham showed a thirty-five percent reduction in crime since the project has been implemented. The project required approval from the home office. The system was derived from a well-organized system that already had procedures for the CCTV system in place and simply expanded on these initial procedures. It is important to make mention of the fact that the police and the surveillance system are two separate entities. The police are notified when an alert has identified an individual. The security department updates the photos every twelve weeks and removes photos that are not currently active wanted individuals. The police submit photos of individuals of interest and the security department enters them into the system.[79] The Security Department of Newham oversees the control room, which conducts the operation of the cameras. There are over three hundred cameras in the Newham system. The Newham system also consists of mobile cameras that directed to different locations to address spikes in crime conditions. The community is an active participant in the system. Newham Security Department has a phone number that the

[78] City of Virginia Beach (2009), *Photosafe Red light Cameras Reduce Red Light Running in Virginia Beach.* Virginia Beach: City of Virginia Beach.
http://www.cops.usdoj.gov/html/cd_rom/tech_docs/pubs/CCTVConstantCamerasTrackVi"CCTV: Constant Cameras Track Violators." Cops.usdoj.gov. NIJ JOURNAL / ISSUE NO. 249.
http://www.cops.usdoj.gov/html/cd_rom/tech_docs/pubs/CCTVConstantCamerasTrackViolators.pdf.

[79] Ibid.

public can call when they want to report suspicious activity. The community involvement and separation from law enforcement creates an atmosphere that can ease any public concern over an Orwellian project. The level of transparency with the public helps to develop a level of trust that was missing with the public in the other case studies.

3. Conclusion

Although the Newham project was operational before the other case studies, it did appear to have the greatest success. The support from the public and the municipality drove much of the success. In the United States, as the communities moved further away from the September 11, 2001, terrorist attack, the concern for privacy and civil liberties and false alerts were issues that weighed on the municipalities. In the initial aftermath, municipalities were completely receptive toward any technology that would provide or enhance security. The United States municipalities were starting both a closed circuit television and facial recognition system together, whereas, the Newham paradigm was supplementing a system that was already developed on a solid framework. The rate of the projects successes increased when the environment was controlled. Whether it was through controlling the chokepoints at the entrance to the Super Bowl venue or mobile cameras in Newham, the ability to identify locations where the technology can thrive and be successfully be applied is important. It does not answer every question a policymaker may have about identifying potential threats, but if properly applied, it will enhance security. It is also important to recognize transparency in implementation can assist policymakers in winning public acceptance.

The next chapter will analyze and access the findings of this research. The conclusions that are drawn will be applied to the solution, which should work toward mitigating the threat of soft target vulnerability.

VI. CONCLUSION, ANALYSIS AND RECOMMENDATION

The intention of this thesis was to create a policy that can maximize the effectiveness of closed circuit television systems by utilizing facial recognition and behavioral recognition software in a proactive manner to both mitigate soft target's vulnerability and prevent crime. Soft targets are everywhere and are difficult to defend. Whether it is a school, movie theater, sports venue or shopping mall, the locations due to their nature of being a gathering place for large groups of the community are targets for both terrorists and criminals.

A. ANALYSIS AND CONCLUSION

The analysis and conclusion centers on four elements that was researched on this matter. The four elements are the technology, deployment of cameras, monitoring and use of personnel and legal political ramifications. The research started out as an effort to see if the technology was ready to operate in a proactive manner, as opposed to the reactive forensic manner in which the technology is currently used. Although there will continue to be the need to utilize the technology in a forensic manner, the research has shown that surveillance systems, such as closed circuit television and emerging technologies like facial recognition and gait recognition can enhance security. In the Super Bowl case study, the data showed that individuals were properly identified by the technology even though arrests were not made at the event. In Newham, the system was attributed with a dramatic reduction in crime.

1. Technology

The research has also shown that the technology cannot just be introduced and projected to be the panacea for all socio-economic and geopolitical problems. In Ybor City, the technology was implemented as part of an extensive revitalization project. It appeared like it had in many municipalities, place the camera and await the crime rate reduction.

When looking at where facial recognition projects have failed, it has generally been through false alerts such as in Virginia Beach. Just as License Plate Readers were placed in strategic locations, it is important to realize a similar process must be used with CCTV and facial recognition. Strategic locations must be determined and a controlled environment must be established.

Another important aspect understands that digital images in the database should continue to be updated. One facet that is not addressed in this research but could be the subject of future studies is the development of biometric identifications. There are states that are currently exploring the process, and it is important to recognize that digital images taken employing the biometric process will only improve the identification rate.

Closed circuit television cameras can be seen in all aspects of society and are continually employing emerging biometrics technology to enhance their capabilities. The research has seen both the success and failure in integrating the technology. There are numerous factors that have led to these successes and failures. The failures were blamed on the technology itself, and although there were cases, such as the one at Virginia Beach where excessive alerts were sent out and blamed on camera failure or improper angle. Lighting that distorted the image was also a cause for failure. It appeared the system was set up to operate on weekends, when the majority of tourism activity occurred. They did have cameras that were inoperable, but it appeared to be a failure to maintain the product on the part of the vendor.[80] Since technology will continue to develop, it is important that the foundation in which it is based must be a firm platform.

The success came about when the technology was implemented in a controlled environment, such as the entrances to Raymond James Stadium in the 2001 Super Bowl. In any security plan the control of entrances or egresses and utilizing these accesses as chokepoints allow security personnel control over who is entering and exiting a venue. It

[80] Duane Bourne, "Facial Recognition Program Flunks Test at Oceanfront."*HamptonRoads.com: Entertainment and Guides for Hampton Roads, VA. The Virginian-Pilot*, 27 Aug. 2007, http://hamptonroads.com/node/317161.

also allows the opportunity to control the physical environment and design structure or create locations that allows for optimal lighting and camera placement for any emerging technology system.

The automated plate reader system, as well as the red light traffic enforcement camera system, has shown the ability to develop a system that can properly image and identify vehicles. In a similar system, just as vehicle alerts can be sent to central control rooms and notifications can be sent from those control rooms to respective law enforcement personnel, emerging technologies can be set up in a comparable manner.

2. Deployment of Cameras

Where the cameras are located is an important aspect of system development. Cameras obstructed by physical architecture or placed at angles that sunlight or other ambient light may impact the image obtained provide neither a forensic or real-time value to any emerging technology. It is important for the agency overseeing the camera deployment to insure that those participating in the system are properly deploying their cameras in an effective manner.

The Ybor City project consisted of thirty-six cameras with all the video feeds going into one control room with one officer monitoring the control room and documenting the alerts. The room was maintained during high pedestrian trafficking times in that particular area. It is necessary to assess the camera placement in order to insure that they are being properly placed to maximize efficiency.

There is a need to provide a framework that will provide oversight, data protection and general guidelines for surveillance systems throughout the country. It is also difficult for the primary stakeholder of the data to have the oversight of it. The stakeholder has a vested interest in the exploitation of the data and not necessarily protection. The data provides a means of proving that the stakeholder is correct in any assessment that the system is working, but the stakeholder also has the ability to minimize the inaccuracies in order to protect the system. The oversight insures that no matter what the outcome individual civil liberties will be protected. The primary stakeholder may not be as concerned about individual liberties, but rather the civil

litigation that may develop from violations of these liberties. There is a system of checks and balances required in order to insure civil liberties a central authority can provide that oversight.

It is important to note that the systems require trained personnel monitoring as well as initially an increase in personnel to respond to alerts. Many of the systems were initially implemented as a means of reducing personnel as opposed to a tool to enhance personnel capabilities. The sole deployment of cameras cannot be expected to eradicate crime and terrorist concerns. The systems will need to be properly integrated, as consideration must also be given to deploying personnel and community resources, even though camera systems can operate and alerts can be set to what may be programmed as suspicious activity.

3. Monitoring and Use of Personnel

The issue becomes an examination of not just this new biometric technology but also that the proper framework and procedures are in place so that future technologies can be easily added to a cohesive framework. A significant part of the framework is that operators are necessary and must be trained to assist in this detection.

In Great Britain, the system was set up where the law enforcement and security service had access to the system, but they were not the primary stakeholders in the operation.[81] In setting up the system in this manner, there will be the elimination of some of the allegations of a secret police conducting surveillance in society. The perception of law enforcement overstepping their boundaries is always a concern in a civil and free society.

4. Legal Political Ramifications

In previous chapters, the discussion reviewed the Handschu ruling in New York City. The Handschu decision transformed the way the New York City Police Department conducted criminal investigations of political groups. Any system that is put in place

81 Terry Honess and Elizabeth Charman, *Closed Circuit Television in Public Places: Its Acceptability and Perceived Effectiveness,* London: Home Office, 1992.

should anticipate concerns of the public perception of the police overstepping their boundaries. A central authority to provide oversight can mitigate some of these concerns by not allowing the police departments to have complete autonomy over the use of the technology.

In major metropolitan areas such as New York City, the multi-jurisdictional element is a significant part of any political effort to control a surveillance system. In New York, the Port Authority controls the airport and the bus terminal, while the Metropolitan Transit Authority has jurisdiction over the commuter railroad except for the part of Pennsylvania Station where Amtrak operates. The area's surrounding all of these transportation facilities is under the jurisdiction of the New York City Police Department. There are surveillance systems in each of these facilities with the ultimate control of the system coordinated by the agency that holds jurisdiction over the geographic area. All across the United States, there are geographical areas faced with similar multijurisdictional elements. It is precisely this multijurisdictional element that will provide a need for an organization to provide oversight. There are policies that may vary between agencies but oversight will provide uniformity in an emerging technology and surveillance system.

In order to develop a successful system, it would appear the current system should be to be re-engineered and a new framework established with oversight. In post-September 11, 2001, America, the effort of expanding surveillance and using any means of technology was initially understandable. The post-September 11 view of seeing the hijackers on surveillance cameras, and the knowledge that they roamed undetected planning their operations, was difficult to understand. Prior to the September 11 attack, facial recognition and closed circuit television systems were emerging as methods to be used in crime reduction strategy.

After September 11, 2001, the technology interest became a method that was used in an effort to prevent future attacks. It appears that the system moved forward without adequately developing a proper framework to integrate the structure. In post-September 11, monies were granted from either state or federal grants to advance both closed circuit television and in some cases, facial recognition or other biometric systems. The fear of

another terrorist attack or of a rising crime rate may have been the motivation, but the integration was left up to the municipality who relied on case law and the advice of vendors of the products explaining and selling the cure for the municipality problem. If we can learn any lesson from the United Kingdom surveillance system, it would be framework and structure of implementation.

In Great Britain, the home office directs the system. The home office provides guidance to the public, even going as far as advice for the consumer of the surveillance product. There are available online applications where an individual can request images that were taken of them in the system.[82] It is precisely this openness and awareness that has made the system successful. It is readily available online where all the cameras were located. If policymakers truly want people to believe protecting the nation is everyone's responsibility, then it is necessary to have some sense of transparency that will avail to the public not only perception that this is all being conducted for their protection but to show it actually is being used for this purpose.

In Tampa Bay, when the ACLU inquired about camera location, they were given various reasons from local authorities as to why these locations could not be released. It can sometimes be as simple as making information available that can eliminate the barriers that can develop between the public watchdogs and the government. The home office in the United Kingdom is the organization that oversees security for the country. The Department of Homeland Security or DHS was set up in the United States to operate on a similar platform providing protection for the homeland. There will need to be an organization that can provide oversight on the surveillance systems and an enforcement arm that will insure that civil rights are not being violated in the process.

82 "Tell Us What You Think of GOV.UK," Request CCTV Footage of Yourself https://www.gov.uk/request-cctv-footage-of-yourself.

B. RECOMMENDATION

Ultimately the recommendation will attempt to provide a platform for the future of surveillance systems throughout the United States. The three issues that are vital to any framework will be the technology, information sharing and the public private partnerships that will be necessary to devise such a system.

1. Technology

Closed circuit television, with facial recognition, is emerging as a model for the future of surveillance. It has gone well beyond the storied past of something written about in novels. There will need to be a new framework instituted that should be similar to the British model but also drawing on successful models that will fit in the United States system. The British are correct on their regulation of the process because individual liberties are assured. There are organizational systems in place that may potentially possess the framework to apply the mission. In the United States, success came in small steps, such as deploying the technology at major events, like the Super Bowl. The effectiveness of the technology, when used in a controlled environment, is an important aspect in protection of soft targets. The common component is the entrance or egress and importance of controlling the environment at these locations is always a factor in a security plan. In order to integrate the system in the current environment, one would have to control the environment. The best integration would be multiple cameras at chokepoints, such as entrances and other egresses to a location.

Another approach is the one used in Newham, England, which deploys mobile cameras in locations where they perceived problems could happen. The New York City Police Department recently introduced Terrahawk Vehicles with Argus surveillance cameras that can be deployed for observation.[83] Not every municipality has this capability, and this is precisely why it is necessary to coordinate public surveillance systems, as they are deployed in order to insure the maximize potential of a system from the outset.

---

83 Andy Cush, "TerraHawk, LLC, "Rapid Response Mobile Surveillance Vehicle. 15 Nov. 2012, http://www.terrahawkllc.com/affiliatesandmedia.html.

The recognition software, although very effective is not effective one hundred percent of the time. The fault usually is generated when camera placement does not allow an effective angle and lighting reflects on the digital image distorting it. It would seem simple enough to solve, but often the systems are being placed in pre-existing structures where the architecture and location of cameras placed do not coincide with the most opportune environment. The technology alone will not resolve the problem. There must also be a method of protecting the data and sharing the information collected with appropriate investigative or necessary agency in need of the information.

2. Information Sharing

The Regional Information Sharing System, or RISS, was previously mentioned as an organization capable of overseeing data protection and information sharing on a national level. It is precisely the type of agency that can provide the framework for management of biometric data and oversight to local authority as how to administer a surveillance program. The local authority understands what its respected needs are and has the established partnerships with local private sector businesses.

When the British Home Office was setting up procedures, the one question that the public always asked was, "What do you want the surveillance system to do?"[84] The local authorities have a better understanding of what type of surveillance system is necessary for their respective communities. They also have the established relationships with local communities to understand what the local needs may be.

Most closed circuit television systems are managed with central control rooms, but the key to success is to have active operators monitoring the system. It is not just a matter of hiring operators because in order to make the system efficiently work there is a need to have trained operators to identify either criminal or terrorist activity. In most United States systems where law enforcement has a managing role in the implementation, officers share a role in monitoring the system. It is understandable in some respects to utilize law enforcement personnel.

84 "Surveillance Camera Code of Practice," Www.gov.uk, June 2013, London: The Stationery Office, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf.

Generally, through their experiences, law enforcement personnel can provide the ability to recognize suspicious behavior or furtive movement that may lead to criminal activity. There is a need to have individuals with these law enforcement experiences involved in some capacity with the training aspect of any potential operators, but operators should not strictly be limited to just law enforcement experiences. The emerging technologies can automatically create an alert, but a trained operator needs to be available to analyze the alert and determine whether or not it necessitates immediate police action or notification to a security service or other agency. The operator needs to be able to recognize the needs of other stakeholders in the system.

The system would also require two other features for the threat to be eradicated. One would be a method of identifying private commercial premises that want to be a partner in the security and protection. In various neighborhoods throughout the country, there are block watch associations. The associations were set up to let anyone coming through the neighborhood know that there were active community members who were watching what was happening in the neighborhood.

3. Public Private Partnership

The British have both public and private security sectors working together. Private sector operators may identify suspicious behavior and will notify the respective operation control room. The operational control room will then notify the respective agency concerned.[85] The Lower Manhattan Security Initiative appears to be a step in the right direction as far as integrating public and private resources, but what works in New York may not necessarily work in Peoria, Illinois. An important aspect of the partnership will be the transparency of the program not only of government agencies but also the public who will be subject to the surveillance system.

The "C.A.T." Program was an example of a successful public-private partnership that allowed police to stop a vehicle after certain hours consenting to a lawful stop by displaying a decal recognized as a participating member. In a similar method, private sector premises will be invited into the Facial Recognition Program in an effort to combat

[85] Ben Brown, *CCTV in Town Centres: Three Case Studies,* no. 68. Police Research Group, 1995.

crime and prevent terrorist activity. A decal can be placed in the window to advise the public of the premise participation in this safety program. The premise cameras can be linked into the system. The current system allows for private system companies to collect biometric data on their own consumers with no guidance as how to secure and protect this data. An agency, such as the RISS, can establish guidelines and procedures on how to protect and secure data. There also will need to be an educational aspect of this organization. By educating the private and public sectors, they are becoming partners in their own security.

In New York City, the crime prevention officers provide this guidance on a daily basis. The crime prevention officers will visit the scene of a burglary and advise victims who have surveillance systems how to better deploy their equipment. It is just another necessary educational aspect that should be part of guidelines provided to the public. The role should be proactive, advising from the outset on how best to deploy systems to prevent criminal activity, or a terrorist act as opposed to reactive to an already developed problem.

In Great Britain, the guidelines set up by the home office ask and answer the questions that the private sector or individuals may need to know the answers to before installing a system. There is always a willingness to blanket an area with cameras but sometimes appropriate and systematic locations can be just as effective. In the United Kingdom, the method of implementing guidelines and procedures regulates the industry. It also provides symmetry to a system that generally is haphazardly organized. The British system relied on trained operators, as well as dividing the workload between the private and public sector. Private sector operators would contact the central control room when they detected evidence of something that would be of concern to the government. The central control room will make a determination as to whether the alert will be disseminated to the police or security service. It would operate in a similar system to the way most current 911-operator systems work.

4. The Ultimate Result

There needs to be an understanding that protecting the homeland is everyone's responsibility both public and private. The protection does not only mean from criminals and terrorists but also a protection of an individual's civil liberties.

This paper has looked at two significant emerging technologies and the effect they can have in enhancing protection, but more importantly, it recognized the need for a central authority to oversee the platform in which these emerging technologies are integrated.

Today, it is behavioral and facial recognition. Tomorrow, it may be a technology that was never imagined before. Either way, it is important to recognize that a structured framework is necessary to facilitate whatever system the future may bring. The goal was to analyze whether the technology was capable of mitigating the vulnerability that exists with soft targets. The vulnerability can be mitigated, but in order to successfully achieve this goal for the long term, the framework of the current system must be re-engineered. It will require a public private partnership synergy with oversight to ensure civil liberties are held in the highest regard.

The intention of this thesis was to create a policy that can maximize the effectiveness of closed circuit television systems by utilizing facial recognition and behavioral recognition software in a proactive manner to both mitigate soft target's vulnerability and prevent crime in New York City. It can be done, but it will require a central authority to provide necessary oversight and insure that all civil liberties are protected in the process.

The ultimate result will be to create a central authority to oversee a dramatically emerging field of technology. The field is developing without legislative influence, but legislation would provide the necessary guidance for municipalities who seek to utilize these evolving technologies in order to enhance security. Congress has created numerous agencies throughout history to provide oversight of various industries. Biometric emerging technology surveillance is an industry that is growing quickly in both the public and private sector. It lacks the monitoring of one central authority. The RISS was created

to provide the ability for law enforcement to share information and protect data and at the same time safeguard individual civil liberties. These are precisely the concerns that overwhelmed past attempts at integrating the technologies. A central authority will allow for that transparency, which is increasingly requested by society. The ultimate result will assure individuals their civil liberties, while providing that effective keen eye to watch over a society and provide the necessary safeguards needed in this post-9/11 world.

BIBLIOGRAPHY

Avexander, David, and Jacob Richert-Boe. “Ethics of Facial Recognition Technology.” http://www.ethicapublishing.com/ethics/4CH11.pdf.

“Back to Basics: Where Did the Video Security System Come From?” *Security Articles and News VinTech Systems,* n.d., n.p. http://www.vintechnology.com/journal /uncategorized/back-to-basics-where-did-the-video-security-system-come-from.

Barrett, L., and S. Gallagher. “What Sin City Can Teach Tom Ridge.” *Baseline,* 32–55, April 2004.

Beddard, R. “Photographs and the Rights of the Individual.” *The Modern Law Review, 58*(6), 771–787, 1995. doi: 10.1111/j.1468-2230.1995.tb02052.x.

Biale, N. Advocacy Coordinator, ACLU Technology and Liberty Program. *You Are Being Watched*, n.d. http://www.youarebeingwatched.us/about/182/.

Bigdeli, A., Lovell, C., Brian, C. Sanderson, T. Shan, and S. Chen. “Vision Processing in Intelligent CCTV for Mass Transport Security.” *Safeguarding Australia Program*, (2007), 1–4.

Bledsoe, W. W., and H. Chan. “A Man Machine Facial Recognition System—Some Preliminary Results, 1965.” Technical Report PRI 19A, Panoramic Research Inc., Palo Alto, CA

Bourne, Duane. “Facial Recognition Program Flunks Test at Oceanfront.” *Virginian-Pilot*, 27 Aug. 2007. http://hamptonroads.com/node/317161.

Buckley, Cara. “New York Plans Surveillance Veil for Downtown.” *New York Times,* 9 July 2007. https://www.fas.org/irp/offdocs/911comm-sec5.pdf.

Button, J. *How London Became the World's CCTV Capital.* July 25, 2005. The Age .COM: http://www.theage.com.au/news/war-on-terror/how-london-became-the-world146s-cctv-capital/2005/07/25/1122143780626.html.

Brown, Ben. *CCTV in Town Centres: Three Case Studies*. No. 68. Police Research Group, 1995.

“CCTV: Constant Cameras Track Violators.” *NIJ Journal*, no. 249 (2003). https://www.ncjrs.gov/pdffiles1/jr000249d.pdf

Commission on Accreditation for Law Enforcement Agencies (CALEA). *Law Enforcement Program: The Standard Manual*, 2011.

California v. Greenwood 486 U.S. 35 (1988).

Cameron, A. K. (2008). *Measuring the Effects of Video Surveillance on Crime in Los Angeles.* California Research Bureau.

Carmondy, Deirdre. "The Subway Anti-Crime Test Abandoned," *New York Times,* October 4, 1985

Carroll, Maurice. "New York City Voters Smile for the Security Cameras, Quinnipiac University Poll," 2013. *Quinnipiac University.* http://www.quinnipiac.edu/institutes-and-centers/polling-institute/new-york-city/release-detail?ReleaseID=1897.

Coll, Steve. "The Super Bowl's Journalism Malfunction." *The New Yorker*. Conde Nast, 5 Feb. 2013. http://www.newyorker.com/online/blogs/comment/2013/02/super-bowl-blackout.html.

"CCTV." *Home*. Transport for London, Aug. 2011. http://www.tfl.gov.uk/assets/downloads/businessandpartners/cctv-guidelines-for-taxis-and-phvs.pdf.

Chicago Police Department. *Crime Surveillance Innovations in Chicago; Law Enforcement and Homeland Security Protection, the History of Police Observation Devices (PODs),* 2008. Chicago: Chicago Police Department.

City of Virginia Beach. *Photosafe Red light Cameras Reduce Red Light Running in Virginia Beach.* Virginia Beach, VA, 2009. http://www.cops.usdoj.gov /html/cd_rom/tech_docs/pubs/CCTVConstantCamerasTrackVideo.

CNN.com. 1 May 2013. CNN|TIME|ORC POLL 5. http://i2.cdn.turner.com/cnn/2013/images/05/01/top5.pdf.

Cush, Andy. "TerraHawk, LLC." Rapid Response Mobile Surveillance Vehicle. 15 Nov. 2012. http://www.terrahawkllc.com/affiliatesandmedia.html.

Cutting, J. E., and L. T. Kozlowski Recognizing Friends by Their Walk: Gait Perception Without Familiarity Cues, *Bulletin of Psychonomic Society,* 1977, 353–356.

Duhigg, Charles. "How Companies Learn Your Secrets." *New York Times,* (2012).

Davenport, J. (2007, September). Tens of Thousands of CCTV Cameras, yet 80% of Crime Unsolved, http://www.thisislondon.co.uk/news/article-23412867-Tens.

"Face Recognition." *Or Face Detection Technology*. N.p., n.d. http://www.engineersgarage.com/articles/face-recognition?page=2.

Fisher, R. A. The Statistical Utilization of Multiple Measurements, Annals of Eugenics, vol. 8 (1938): 376–386.

Forrest Lee. "Someone's Watching You: From Microchips in Your Underwear to Satellites Monitoring Your Every Move, Find Out Who's Tracking You and What You Can Do About It," 2011, Adams Media Corporation.

Franken, Al, Senator. "What Facial Recognition Technology Means for Privacy and Civil Liberties."*View a Hearing or Meeting*. Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law, 18 July 2012.

Fussey, P. An Interrupted Transmission. *Surveillance & Society, Processes of CCTV Implementation and the Impact of Human Agency* (Special Issue on Surveillance and Criminal Justice), 229–256, 2007.

Gates, Kelly A. *Our Biometric Future-Facial Recognition Technology and the Culture of Surveillance*. New York City: New York University, 2011.

Gill, Martin and Angela Spriggs. *The Impact of CCTV: Fourteen Case Studies*, Home Office Report 15/05.

———. *Assessing the Impact of CCTV*, 2005. http://www.securitymanagement.com/archive/library/cctv_news0505.pdf.

GoldStein, A. J., L. D. Harmon, and A. B. Lesk. "Identification of Human Faces." *Proc IEEE* 59, no. 5 (1971): 748–760.

Grass, M. L. The Legal Regulation of CCTV in Europe. *Surveillance & Society*, 14, 2004.

Greenberg, David F., and Jeffrey B. Roush. "The Effectiveness of an Electronic Security Management System in a Privately Owned Apartment Complex."*Evaluation Review* 33, no. 1 (2009): 3–26.

Gwendolyn, Brandon, ed."National Evaluation of CCTV: Early Findings on Scheme Implementation – Effective Practice Guide." Brandon Gwendolyn, ed., Home Office Development and Practice Report., June 2003. http://www.no-cctv.org.uk/docs/Scarman_Centre(HO)-NationalEvaluationCCTV-early_findings.pdf.

HANDSCHU v. Special Services Division 288 F.Supp.2d 411.

Honess, Terry, and Elizabeth Charman. *Closed Circuit Television in Public Places: Its Acceptability and Perceived Effectiveness*. London: Home Office, 1992.

Honovich, J. (2008). Is Public CCTV Effective. *IP Video Market Info*, 7. http://ipvideomarket.info/report/is_public_cctv_effective.

The Internet Classics Archive | On the Gait of Animals by Aristotle." *The Internet Classics Archive | On the Gait of Animals by Aristotle*. Trans. A. S. L. Farquharson. MIT, n.d. Web. 20 Nov. 2013. http://classics.mit.edu/Aristotle/gait_anim.html.

Kale A., R. Chowdhury, and R. Chellappa. Towards a View Invariant Gait Recognition Algorithm, University of Maryland, 2004, 1–8.

Kale, A., A. N. Rajagopalan, N. Cuntoor, and V. Kruger University of Maryland, 2002, *Gait-based Recognition of Humans Using Continuous HMMs*.

Katz vs. United States 389 U.S. 347 (1967).

Kean, Thomas, Lee Hamilton, R. Ben-Veniste, B. Kerrey, F. Fielding, J. Lehman, J. Gorelick, T. Roemer, S. Gorton, and J. Thompson. "National Commission on Terrorist Attacks Upon the United States." *Washington DC* (2004). https://www.fas.org/irp/offdocs/911comm-sec5.pdf.

Kyllo v. United States 533 U.S. 27 (2001). http://laws.findlaw.com/us/533/27.html.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. Los Angeles: SAGE/CQ, 2012.

Lockie, Mark. "NBSP to Commence Testing Programme." *Biometric Technology Today* (2006).

McCahill, M., and C. Norris. CCTV In Britain. *Urban Eye*, *3*(March), 70, 2002.

———. CCTV In London. *Urban Eye, Analyzing the Employment of CCTV in European Cities and Assessing Its Social and Political Impacts.* June 31, 2002.

Miller, J. Why New York Hasn't Been Attacked Again. *Telegraph.Co.UK*, 2007. http:/www.telegraph.co.uk/comment/personal-view/3642611/why-new-york-hasnt-been-attacked-again.html.

Nestel, T. (2006). *Using Surveillance Camera Systems to Monitor Public Domains: Can Abuse Be Prevented.* Master's thesis, Naval Postgraduate School.

Niccolai, J. *Closed Circuit TC May Aid London Bombing Investigation*, July 8, 2005, http://www.infoworld.com/t/networking/closed-circuittv-may-aid-london-bombing-investigation-835.

Nieto, M., K. Johnson-Dodds and Charlene Wear Simmons, PhD (2002). *Public and Private Applications of Video Surveillance and Biometric Technologies,* http://www.library.ca.gov/crb/02/06/02-006.pdf.

Niyogi, S. A., and E. H. Adelson. Analyzing Gait with Spatiotemporal Surfaces. In Proc. of IEEE Workshop on Non-Rigid Motion, 24–29, 1994.

Norris, Clive. *Surveillance, Closed Circuit Television and Social Control* (vol. NCJ 178396): National Criminal Justice Service, 1998.

Norris, Clive, and Gary Armstrong. *The Maximum Surveillance Society: The Rise of CCTV*. Oxford: Berg, 1999.

Phillips, P. Jonathon. *FERET (Face Recognition Technology) Recognition Algorithm Development and Test Results*. Army Research Laboratory, 1996.

———. "*Face Vendor Recognition Test.* National Institute of Standards and Technology, n.d., http://www.nist.gov/itl/iad/ig/frvt-home.cfm.

Ratcliffe, J. *Video Surveillance of Public Places.* Washington DC: United States Department of Justice Community Oriented Police Services, 2006.

"Regional Information Sharing Systems (RISS)." http://www.riss.net/.

Schwabe, William, Lois M. Davis, and Brian A. Jackson. Challenges and Choices for Crime-Fighting Technology Federal Support of State and Local Law Enforcement. Santa Monica, CA: RAND Corporation, 2001. http://www.rand.org/pubs/monograph_reports/MR1349.

Shah, Rajiv, and Jeremy Braithwaite. *Spread Too Yhin: Analyzing the Effectiveness of Chicago Camera Network on Crime*, Police Practice and Research: An International Journal, April 2012.

Sims, Jennifer E., and Burton L. Gerber. *Transforming U.S. Intelligence*. Washington, D.C.: Georgetown UP, 2007.

Sirovich, L., and M. Kirby. "Low-dimensional Procedure for the Characterization of Human Faces," *J. Opt. Soc. Am.* A**4**, (1987): 519–524.

Smith, James. “Candid Camera: CCTV and the Value Of Situational Awareness.” *Asia Pacific Future Gov*. (2006). http://www.futuregov.asia/articles/2006/jan/05 /candid-camera-cctv-and-value-situational-awareness/.

“Surveillance Camera Code of Practice.” Www.gov.uk. June 2013. London: The Stationery Office. https://www.gov.uk/government/uploads/system/uploads /attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf.

“Tampa Police Department Installs Visionics' FaceIt Technology in Anti-crime CCTV Initiative - L-1 Identity Solutions.” *Tampa Police Department Installs Visionics' FaceIt Technology in Anti-crime CCTV Initiative - L-1 Identity Solutions*. Visionics Corporation, 29 June 2001, http://ir.l1id.com/releasedetail.cfm?ReleaseID=208637.

“Tell Us What You Think of GOV.UK.” Request CCTV Footage of Yourself, http://digital.cabinetoffice.gov.uk/. 22 Nov. 2013 https://www.gov.uk/request-cctv-footage-of-yourself.

Terry v. Ohio, 392 U.S. 1 (1986).

Thompson, Richard M. “Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses.” Congressional Research Service, Library of Congress, 2012.

United States. Combating Terrorism Technical Support Office. Technical Support Working Group. *Best Practices for the Retrieval of Video Evidence from Digital CCTV Systems*. Version 1.0. Arlington, VA: Technical Support Working Group, 2006.

U.S. General Accounting Office. Video Surveillance Information on Law Enforcement Use, Richard M. Stana, June 2003.

“Welcome.” *Biometrics.gov*. NSTC Subcommittee on Biometrics and Identity Management, 6 Aug. 2006, http://www.biometrics.gov/.

Welsh, B. C., and D. P. Farrington. Evidence-Based Crime Prevention: The Effectiveness of CCTV. *Crime Prev Community Saf*, *6*(2), 21–33, 2002b.

———. “Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis,” *Justice Quarterly*, vol. 26, 2009.

———. Effects of Closed Circuit Television Surveillance on Crime. *Campbell Systematic Reviews* (2008): 17.

———. Crime Prevention Effects of Closed Circuit Television: A Systematic Review. *Home Office Research Study, 252*, 68 2002a.

Woodward, John D. Jr. et al. *Biometrics: A Look at Facial Recognition*. RAND CORP Santa Monica CA, 2003.

———. *Super Bowl Surveillance: Facing Up to Biometrics*. Rand Arroyo Center, Santa Monica CA, 2001.

"Ybor Story."*Welcome to Ybor City*. Ybor City, Florida Chamber of Commerce, 2011, http://www.ybor.org/ybor-story.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California