NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

FACING REALITY: THE BENEFITS AND CHALLENGES OF FACIAL RECOGNITION FOR THE NYPD

by

Anthony M. Carter

September 2018

Co-Advisors: Lauren Wollman (contractor)
Carolyn C. Halladay

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 September 2018	3. REPORT TYPE AND DATES COVERED Master's thesis

4. TITLE AND SUBTITLE FACING REALITY: THE BENEFITS AND CHALLENGES OF FACIAL RECOGNITION FOR THE NYPD	5. FUNDING NUMBERS
6. AUTHOR(S) Anthony M. Carter	
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.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	12b. DISTRIBUTION CODE A

13. ABSTRACT (maximum 200 words)

Facial recognition technology (FRT) and license plate readers (LPRs) are comparable technologies that share similar benefits and challenges. Many of the challenges associated with LPRs have already been mitigated, resulting in citizen acceptance and expanded use. Recent advancements in FRT, such as its use in real time, create new opportunities to leverage the technology for increased public safety. To what extent are LPRs and FRT analogous, and how can the use of LPRs by the New York City Police Department (NYPD) provide a roadmap for public support of real-time FRT? This thesis examines benefits and challenges that may arise if the NYPD considers using real-time FRT in the New York City subway system. Through comparative analysis, this thesis determines that real-time FRT could help law enforcement deter terrorism, prevent violent crime, identify wanted individuals, find missing persons as well as assist in mental health situations and post-event investigations. Real-time FRT can help the NYPD meet its mission by reducing fear, increasing resiliency, and adding a layer of protection for citizens riding in the New York City subway system.

14. SUBJECT TERMS facial recognition, facial recognition technology, FRT, real-time facial recognition technology, New York City Police Department, NYPD, license plate readers, police technology, LPR	15. NUMBER OF PAGES 123
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	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.

FACING REALITY: THE BENEFITS AND CHALLENGES OF FACIAL RECOGNITION FOR THE NYPD

Anthony M. Carter
Deputy Inspector, New York City Police Department
BS, The State University of New York, Empire State College

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
September 2018

Approved by: Lauren Wollman
Co-Advisor

Carolyn C. Halladay
Co-Advisor

Erik J. Dahl
Associate Chair for Instruction,
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Facial recognition technology (FRT) and license plate readers (LPRs) are comparable technologies that share similar benefits and challenges. Many of the challenges associated with LPRs have already been mitigated, resulting in citizen acceptance and expanded use. Recent advancements in FRT, such as its use in real time, create new opportunities to leverage the technology for increased public safety. To what extent are LPRs and FRT analogous, and how can the use of LPRs by the New York City Police Department (NYPD) provide a roadmap for public support of real-time FRT? This thesis examines benefits and challenges that may arise if the NYPD considers using real-time FRT in the New York City subway system. Through comparative analysis, this thesis determines that real-time FRT could help law enforcement deter terrorism, prevent violent crime, identify wanted individuals, find missing persons as well as assist in mental health situations and post-event investigations. Real-time FRT can help the NYPD meet its mission by reducing fear, increasing resiliency, and adding a layer of protection for citizens riding in the New York City subway system.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
- A. RESEARCH QUESTION 2
- B. OVERVIEW OF FACIAL RECOGNITION TECHNOLOGY 2
- C. UNINTENDED CONSEQUENCES OF BODY-WORN CAMERAS 5
- D. LITERATURE REVIEW 11
  - 1. Privacy versus Security 11
  - 2. Transparency 19
- E. RESEARCH DESIGN 23
- F. CHAPTER OUTLINE 24

II. LICENSE PLATE READERS 25
- A. OVERVIEW 25
  - 1. History of License Plate Reader Technology 25
  - 2. How License Plate Readers Work 28
- B. BENEFITS OF LPR TECHNOLOGY 30
  - 1. Crime Prevention Benefits 30
  - 2. Law Enforcement and Public Benefits 34
- C. CHALLENGES 37
  - 1. Privacy 38
  - 2. Accuracy 41
  - 3. Transparency and Public Trust 43
- D. CONCLUSION 46

III. FACIAL RECOGNITION TECHNOLOGY 49
- A. OVERVIEW 49
- B. BENEFITS OF FRT 50
  - 1. Crime Prevention Benefits 53
  - 2. Law Enforcement and Public Benefits 59
- C. CHALLENGES 64
  - 1. Privacy 65
  - 2. Accuracy 73
  - 3. Transparency and Public Trust 75
- D. CONCLUSION 77

IV. CONCLUSION 79

LIST OF REFERENCES **85**

INITIAL DISTRIBUTION LIST **101**

LIST OF FIGURES

Figure 1. Notional Large-Scale, Integrated Departmental LPR Setup.....29

Figure 2. Algorithm for Matching Facial Images.....51

Figure 3. How FRT Systems Generally Work 53

Figure 4. The Gateless Gate Line Concept Using FRT.....62

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Comparison of Benefits of LPRs, FRT, and BWCs 82

Table 2. Comparison of Challenges with LPRs, FRT, and BWCs 83

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACLU	American Civil Liberties Union
BWC	body-worn camera
CCTV	closed-circuit television
CPOP	community patrol officer program
CUFPR	Communities United for Police Reform
DAS	domain awareness system
DHS	Department of Homeland Security
DMV	Department of Motor Vehicles
FBI	Federal Bureau of Investigation
FIS	Facial Identification Section
FRT	facial recognition technology
ICE	Immigration and Customs Enforcement
INTERPOL	International Police
KRVS	known-risk vehicle stop
LMSI	Lower Manhattan Security Initiative
LPR	license plate reader
MTA	Metropolitan Transit Authority
NYPD	New York City Police Department
OPM	Office of Personnel Management
SQF	stop, question, and frisk
VRA	vehicle-ramming attack

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Facial recognition technology (FRT) is a biometric technology that—if the New York City Police Department (NYPD) implements it in the New York City subway system—could have significant benefits of preventing violent crime, deterring terrorism, helping investigate past crimes, locating missing persons, providing assistance to individuals with special needs, and integrating with other technology platforms to allow for greater efficiencies in policing. Since the NYPD successfully uses license plate reader (LPR) technology to increase public safety with an existing legal and policy framework governing its use, and because FRT is similar to LPR technology—in terms of law enforcement use of the technology as well as benefits and challenges—this thesis presents a comparative analysis of the two technologies.

From this analysis, the following questions can be answered: To what extent are LPRs and FRT analogous, and how can the NYPD's use of LPRs provide a roadmap for public support of real-time FRT? Currently, the NYPD does not use automatic or real-time FRT, but specially trained detectives assigned to the Facial Identification Section use FRT to investigate past crimes and assist detectives in the field. Other law enforcement agencies outside the United States, however, are using or evaluating the effectiveness of real-time FRT, which has significantly improved in recent years, in part because of the development of high-definition video, advancements in storage capabilities, and the ability to evaluate faces in real time. Modern FRT systems can also recognize an individual with varying facial expressions. Therefore, a person can be accurately identified in a facial recognition database, even if the facial expression is different from the original image contained in the database.

Communities benefit from LPR technology, despite privacy concerns and the contention of critics, such as the American Civil Liberties Union, which assert that law enforcement agencies should not be able to collect and store information on law-abiding

citizens who are not suspected of criminal wrongdoing.[1] This thesis proposes that although privacy considerations may exist, the benefits of LPR technology outweigh these concerns. LPRs and FRT are similar types of technologies that perform similar functions. They both scan the image of an unknown variable and attempt to match it against a known variable contained in a database, collecting all information—without bias—on license plates or persons. Furthermore, both technologies use "hot lists," which compare the scanned image against information or images contained in local, state, and federal databases. Computer software then compares the scanned image against collected data or images. Finally, the information, such as images of a stolen vehicle or wanted person, received from both technologies requires human verification. Like LPR technology, FRT—especially when used in real time—has significant benefits and can act as a force multiplier for limited NYPD resources in crowded environments such as the New York City subway system.

The NYPD has developed sound policies with LPRs and has already mitigated the challenges to minimize potential harm due to misuse and violation of civil liberties. In addition, LPRs are generally acknowledged as a common and publicly accepted law enforcement technology, largely in part because the NYPD proactively addressed many of the risks. The NYPD addressed LPR data collection, retention, and sharing through robust and clear policies. In addition, the police department addressed potential misuse of LPRs to eliminate their ambiguities and clearly define acceptable practices. Through comparative analysis, this thesis determines that real-time FRT could help law enforcement deter terrorism, prevent violent crime, identify wanted individuals, find missing persons, and assist in mental health situations and post-event investigations. This thesis also addresses the litany of challenges in the use of FRT—privacy concerns as well as false positives, false negatives, intentional circumvention of real-time FRT, and law enforcement misappropriations—and identifies the concerns over how law enforcement collects, shares, and disseminates personal information obtained from facial recognition software. This thesis concludes that real-time FRT can help the NYPD meet its mission by reducing fear,

[1] Ben Eisler, "ACLU Concerned Automatic License Plate Readers May Invade Privacy," WJLA News, July 30, 2012, http://wjla.com/news/local/aclu-concerned-red-light-cameras-may-invade-privacy-78301.

increasing resiliency, and adding a layer of protection for citizens riding in the New York City subway system.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I owe my deepest debt and gratitude to my wife and amazing children. I can never thank all of you enough for your love, support, and understanding over the last 18 months. Also, to Mom and Dad, thank you for your guidance, continuous support, and love over the last 40-plus years.

Thank you, Police Commissioner James O'Neill and First Deputy Commissioner Benjamin Tucker for allowing me to participate in this most prestigious program. Thank you, Chief Terence Monahan, Deputy Chief Frank Vega, and Assistant Chief Michael Lipetri, for your continued support during my extended absences throughout this program. To my advisors, Carolyn Halladay and Lauren Wollman, you both were instrumental during the thesis process and in furthering the depth of my argument through countless emails, calls, and text messages. You helped me focus on the importance of this project. Also, thank you to my writing coaches—Carla Orvis Hunt, Cheryldee Huddleston, and Noel Yucuis—for all your support and guidance.

I am extremely grateful to the Naval Postgraduate School and the Center for Homeland Defense and Security for accepting me into this program. I will treasure the knowledge, the memories, and the excellence that has become a part of who I am.

Thank you to all of my classmates. I will miss being surrounded by some of the most intelligent and accomplished individuals I have ever met. My greatest experiences in learning about homeland security came from you. Thank you all for your contributions to the security and safety of this great country.

Finally, to the men and woman of the New York City Police Department, I thank you all for what you do each and every day. I am truly grateful to be considered a member of the greatest police department in the world, and it is an honor to walk among you. Stay safe, and God bless.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Law enforcement organizations around the world are using real-time facial recognition technology (FRT) to identify known terrorists, apprehend wanted perpetrators, and locate missing persons. Law enforcement agencies in Europe are also piloting real-time FRT for use in parades, sporting events, and subway systems. For example, the Metropolitan Police in London recently used real-time FRT at the Notting Hill Carnival to identify and arrest wanted criminals, quelling the violence that has marred the event in previous years.[1] Biometric technology is advancing rapidly, allowing law enforcement agencies to use real-time FRT with any device equipped with a camera, such as cell phones, fixed cameras, mobile cameras, body-worn cameras (BWCs), and drones. In China, the use of real-time FRT by law enforcement has proven successful. For example, in Zhengzhou, facial recognition identified a drug smuggler, and in Wuhu, facial recognition cameras identified a murder suspect buying food from a street vendor.[2] Such examples from various parts of the world illustrate that FRT, especially when used in real time, has significant public benefits, despite several concerns associated with its use.

FRT is a biometric technology that—if considered by the New York City Police Department (NYPD) for use in the New York City subway system—could have the significant benefits of preventing violent crime, deterring terrorism, investigating past crimes, locating missing persons, providing assistance to individuals with special needs, and integrating with other technology platforms to allow for greater efficiencies in policing. Currently, a knowledge gap exists in the NYPD and other law enforcement organizations for successful implementation of real-time FRT. The NYPD needs to examine the benefits, challenges, cost, and overall effectiveness thoroughly, prior to adopting FRT for real-time use. The possibility exists that FRT is similar to LPR technology in terms of how law

---

[1] Vikram Dodd, "Met Police to Use Facial Recognition Software at Notting Hill Carnival," *Guardian*, August 5, 2017, http://www.theguardian.com/uk-news/2017/aug/05/met-police-facial-recognition-software-notting-hill-carnival.

[2] Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras," *New York Times*, July 9, 2018, https://www.nytimes.com/2018/07/08/business/china-edsurveillance-technology.html.

enforcement uses the technology, as well as respective benefits and challenges of both technologies. The NYPD successfully uses license plate reader (LPR) technology and has an existing framework that governs its use. In addition, both technologies have similar crime prevention benefits and are operationally analogous because they can scan an unknown image and compare it against known faces or license plates contained in a database.

The NYPD continuously evaluates new technologies that may further its ability to keep citizens safe, deter crime, and prevent acts of terrorism. Using real-time FRT may provide additional layers of protection against known criminals and/or terrorist threats. Controlled access, lighting, environmental factors, and an existing network of cameras make the New York City subway system an ideal location for the use of real-time FRT. This thesis examines LPRs and FRT to test the idea that both technologies are in fact similar, so a similar framework for real-time FRT can be adopted.

A. RESEARCH QUESTION

To what extent are LPRs and FRT analogous, and how can the NYPD's use of LPRs provide a roadmap for public support of real-time FRT?

B. OVERVIEW OF FACIAL RECOGNITION TECHNOLOGY

Kelly Gates defines *real time* as "making the outcome of mediated processes happen immediately."[3] Gates adds that FRT, when used in real time, "involves a complex technical process of detecting faces in video feeds, grabbing them from the image, segmenting them from the background clutter, applying an algorithm to translate those images into a digital template or 'faceprint,' and then searching that template against databases of archived photographs."[4] Real-time identification happens instantly, making real-time use of FRT an attractive feature for law enforcement. Currently, the NYPD has specially trained detectives assigned to its Facial Identification Section (FIS), which uses

[3] Kelly Gates, "Identifying the 9/11 'Faces of Terror,'" *Cultural Studies* 20, no. 4/5 (September 7, 2006): 426, https://doi.org/10.1080/09502380600708820.

[4] Gates, 426.

FRT to investigate past crimes and provides resources to detectives in the field. The NYPD does not use automatic, or real-time, FRT in any capacity. Other law enforcement agencies outside the United States, however, are using real-time FRT for subway passenger identification, transportation payment, crime fighting, access control into transit facilities, and terrorism mitigation.[5]

FRT has significantly improved in recent years in part because of the development of high-definition video and advancements in storage capabilities, pushing vast quantities of information into the cloud.[6] Modern FRT systems can also recognize an individual with varying facial expressions—even expressions of anger, disgust, fear, happiness, sadness, or surprise.[7] An individual can be correctly identified in a facial recognition database despite having facial expressions different from the original image contained in the database. In addition, software companies integrate mobile applications to synchronize with FRT software.[8] Such integrations create new purposes for FRT.

The RAND Corporation defines biometrics as "any automatically measurable, robust and distinctive characteristic or personal trait that can be used to identify an individual or verify the claimed identity of an individual."[9] FRT processes and matches unique characteristics for identification or authorization. The technology uses a digital or video camera to detect images of an unknown individual, analyzes the features within the

---

[5] The Shanghai Metro has 367 stations and moves approximately 10.6 million passengers daily. Shanghai Shentong Metro Group, in conjunction with Ant Financial Services Group, announced that it will soon install facial recognition at station entrances. Bien Perez, "Shanghai Subway to Use Alibaba Voice and Facial Recognition Technologies," *South China Morning Post*, December 5, 2017, http://www.scmp.com/tech/enterprises/article/2123014/shanghai-subway-use-alibaba-voice-and-facial-recognition-systems-ai.

[6] Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*, Special Publication 800–145 (Gaithersburg, MD: NIST, September 2011), 2, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[7] Shubhada Deshmukh, Manasi Patwardhan, and Anjali Mahajan, "Survey on Real-Time Facial Expression Recognition Techniques," *IET Biometrics* 5, no. 3 (September 2016): 162.

[8] "Biometrica Announces Release of New SSIN, with Mobile App That Allows Near Real-Time Facial Recognition," Biometrica Systems, November 23, 2016, https://biometrica.com/biometrica-announces-release-of-new-ssin-with-mobile-app-that-allows-near-real-time-facial-recognition/.

[9] John D. Woodward Jr. et al., *Biometrics: A Look at Facial Recognition* (Santa Monica, CA: RAND Corporation, 2003), 1, http://www.dtic.mil/dtic/tr/fulltext/u2/a414520.pdf.

image, and compares them with images of known individuals contained in the database.[10] Two different methods enable the use of FRT. The first method relies on "criteria like the distance between your eyes, the measurements of your nose, lips and other facial features and matches them against an existing database."[11] The second method "looks at points of interest on the face and tracks how the pixels in a photograph cluster to form a person's nose."[12] Facial recognition is similar to other biometrics, such as fingerprints, iris scans, and voice recognition, because these technologies begin with an unknown variable, which they attempt to identify.

Fifty years since the inception of their use, FRT and other biometrics have integrated with existing technologies, such as cellular phones and digital photo albums, so people are more accustomed to the technology—which may help the NYPD garner more public acceptance of FRT's benefits and efficiencies. Just as technology companies, such as Google, Amazon, Facebook, and Apple, are leveraging FRT, so, too, are law enforcement organizations. Law enforcement has begun to apply FRT in ways that contrast starkly with the technology's original use of preventing terrorism.

Citizens continue to fear threats of terrorism when moving around public places and often look to uniformed police officers to protect them from harm. Kelly Gates argues that automated FRT was born in the wake of 9/11, with the entire country looking for a "high-tech" method to identify and deter terrorists.[13] Gates also argues that supporters of biometric technologies used the war on terror to identify new initiatives for redefining citizen expectations of homeland security. As stated by British sociologist Andrew Barry, the United States was obsessed with finding any and all available technological solutions.[14]

---

[10] "Facial Recognition," Find Biometrics, Global Identity Management, accessed August 7, 2018, https://findbiometrics.com/solutions/facial-recognition/.

[11] Stacy Higginbotham, "Facial Recognition Freak Out: What the Technology Can and Can't Do," *Fortune*, June 23, 2015, http://fortune.com/2015/06/23/facial-recognition-freak-out/.

[12] Higginbotham.

[13] Kelly Gates, "Identifying the 9/11 'Faces of Terror,'" 418.

[14] Gates, 423.

New York is the largest city in America and is home to one of the most extensive and safest subway systems in the world.[15] Terrorists, however, have successfully targeted New York City three times since September 2016, and those wishing to plan attacks continue to view it as a primary target. In addition to the NYPD's daily responsibility to reduce crime, the continuous undertaking to prevent a large-scale terror attack in the subway system has never been more significant. New York City subway facilities are often overcrowded, particularly during peak times, making it virtually impossible to screen every passenger entering the station.[16] Approximately six million people navigate their way through 472 stations inside thousands of packed subway cars each day.[17] The massive volumes of people who traverse the New York City subway system daily make trains and platform areas attractive targets for terrorists.

On the other hand, if the NYPD uses FRT as a real-time solution in the New York City subway system, several obstacles exist, such as privacy concerns, public trust challenges, and the overall reliability of the technology. Real-time FRT can become part of an all-encompassing policing strategy, but its implementation in the New York City subway system is not the magic bullet for reducing violent crime or preventing a terror attack. It could be, however, an additional tool for the NYPD to use for the ever-changing challenges of policing the nation's largest subway system.

C. UNINTENDED CONSEQUENCES OF BODY-WORN CAMERAS

In major cities around the world, police departments are harnessing BWC technology to video record police interactions with citizens. A BWC is typically worn by a police officer for recording the audio and video of encounters, as well as evidence searches. BWCs allow others to evaluate the actions of a police officer or citizen based on

---

[15] Lisa Anderson, "Exclusive-Poll: New York City Transport Seen as Safest in World for Women," Reuters, October 28, 2014, https://uk.reuters.com/article/women-poll-newyork/exclusive-poll-new-york-city-transport-seen-as-safest-in-world-for-women-idUKL6N0SB4WI20141029.

[16] Emma G. Fitzsimmons, "Every New York City Subway Line Is Getting Worse. Here's Why," *New York Times*, June 28, 2017, https://www.nytimes.com/interactive/2017/06/28/nyregion/subway-delays-overcrowding.html.

[17] "Introduction to Subway Ridership," Metropolitan Transportation Authority, accessed September 4, 2017, http://web.mta.info/nyct/facts/ridership/.

video footage collected from one or more officers. The NYPD is in the process of completing the implementation of BWCs and will soon equip every police officer, detective, sergeant, and lieutenant working on the street.[18] Since the implementation of BWCs in 2014, differing opinions exist on their success and the over-arching benefit to both citizens and police officers. Advocacy groups are still collectively debating LPR and BWC use by law enforcement, but BWCs and LPRs serve different purposes and have separate challenges for law enforcement, and therefore, decision-makers should not draw comparisons.

BWCs were seen by many as a panacea to hold officers accountable for police use-of-force encounters and to provide transparency in policing, thereby enabling stronger community relations between law enforcement and citizens. Their use, however, has created issues due to the high costs of BWC programs and high-profile controversies between law enforcement and citizens, due to policy inconsistencies from one police department to the next. For example, some departments readily release BWC videos to the public while others are more restrictive in releasing them. BWCs were supposed to remove the ambiguity of policing, create an environment where policing is transparent, improve relations between police and the community, and decrease civilian complaints against police officers and use-of-force incidents.

Various surveillance technologies, such as video cameras, have been around for over 50 years. In the last two decades, video cameras have become ubiquitous—because of their price and quality—and often integrated with other devices such as smartphones. Just as the use of LPR technology by law enforcement has rapidly expanded within a short period, both law enforcement decision-makers and critics quickly accepted BWC technology as a panacea to attain greater transparency and accountability between police officers and citizens. Police-involved use of force—beginning with the death of Eric Garner in Staten Island, New York, and followed by the heavily scrutinized deaths of Michael Brown in Ferguson, Missouri, and Freddie Gray in Baltimore, Maryland—set off

[18] Rebecca Savransky, "De Blasio: NYPD Planning to Have Body Camera on Every Cop by Year's End," *The Hill*, January 31, 2018, http://thehill.com/homenews/state-watch/371582-de-blasio-says-nyc-planning-to-have-every-cop-equipped-with-body-camera.

violent protests throughout the country. A citizen observing the confrontation, arrest, and subsequent death of Eric Garner captured the incident on video. There are often questions about police-related interactions captured on video and posted on social media sites for citizens to critique. Sometimes, video footage clearly captures officer misconduct, such as the police-involved shooting of Walter Scott, an unarmed man following a traffic stop, by a South Carolina police officer. Other videos capturing police action raise more questions than answers. In Louisville, Kentucky, BWCs captured the aftermath of a vehicle collision, resulting in the deaths of Isaiah Basham and Lexi Grey. Questions about whether the officers were engaged in a vehicle pursuit are inconclusive based on BWC footage. Scott Greenwood of the American Civil Liberties Union (ACLU) argues that many police encounters are already recorded in a variety of ways. At a 2013 conference, he spoke in favor of BWCs:

> The average interaction between an officer and a citizen in an urban area is already recorded in multiple ways. The citizen may record it on his phone. If there is some conflict happening, one or more witnesses may record it. Often there are fixed security cameras nearby that capture the interaction. So the thing that makes the most sense—if you really want accountability both for your officers and for the people they interact with—is to also have video from the officer's perspective.[19]

A BWC varies in size, specifications, quality, and durability, just as in commercially sold video cameras. The location on a police officer's body where a BWC is mounted depends on the size and shape of the equipment. The most significant difference between closed-circuit television (CCTV) cameras and BWCs is the direct involvement of the police officer and his actions. Passive CCTV recordings are not reviewed or retained for a prolonged period unless a specific incident necessitates their review and preservation. BWCs, however, record active engagement between an officer and citizen, capturing up-close, high-quality audio and video of specific interactions.

There are privacy and community concerns associated with the use of BWCs. Policy issues for BWCs often involve the effects of privacy, community relations, overall

---

[19] Lindsay Miller and Jessica Toliver, *Implementing a Body-Worn Camera Program: Recommendations and Lessons Learned* (Washington, DC: Community Oriented Policing Services, 2014), 1, https://www.justice.gov/iso/opa/resources/47201491213471524686 9.pdf.

cost, court testimony, and concerns raised internally by officers wearing the technology. Demonstrating the most significant difference between fixed cameras and BWCs, officers wearing the latter often enter private residences and other locations not accessible to the public. When officers activate their cameras, their decisions need to conform to the requirements set forth by their respective departments, while striking a balance between transparency and individual privacy.[20] Additional privacy concerns with BWCs involve how the footage is stored, used, and shared—particularly when footage captures images of a private or personal nature.[21] Sir Hugh Orde, president of the Association of Chief Police Officers (UK), explains the importance of effective policies involving BWCs:

> Legitimacy in policing is built on trust. And the notion of video-recording every interaction in a very tense situation would simply not be a practical operational way of delivering policing. In fact, it would exacerbate all sorts of problems. In the United Kingdom, we're also subject to human rights legislation, laws on right to privacy, right to family life, and I'm sure you have similar statutes. It's far more complicated than a blanket policy of "every interaction is filmed." I think that's far too simplistic. We have to give our officers some discretion. We cannot have a policy that limits discretion of officers to a point where using these devices has a negative effect on community–police relations.[22]

In some states, the law mandates that officers obtain consent from an individual prior to activating a BWC. For the NYPD, the patrol guide defines specific rules and regulations that every officer must follow and dictates precisely when an officer should activate a BWC. Officers must activate their BWCs when ShotSpotter—a technology that uses sensors and software—identifies gunfire, during interior vertical patrols of New York City Housing Authority buildings, or in anticipation of a citizen interaction to capture the incident in its entirety. The NYPD acknowledges, however, that BWCs do not capture all encounters and may not clearly depict the complete incident. The NYPD prohibits BWC recordings of interviews with confidential informants or victims of sex crimes, during strip

[20] Miller and Toliver, 11.

[21] Miller and Toliver, 11.

[22] Miller and Toliver, 14.

searches, while inside courthouses (except when lodging a prisoner), and inside medical facilities.[23]

Such policies, although required by law, fail to capture some police encounters with citizens. On June 30, 2017, Henry Bello, a disgruntled doctor, walked into Bronx Lebanon Hospital armed with an AR-15 assault rifle and ascended to the 16th and 17th floors, where he began shooting randomly, killing one and wounding six before taking his own life. Notably, because BWCs do not capture all incidents, no single technology exists that can address all police and citizen concerns. Privacy laws prevent police officers from recording inside hospitals and, therefore, BWCs would not have captured the shooting or its aftermath. Therefore, an assessment of police tactics during this active-shooter incident could not have been evaluated using BWC video footage.

Psychologists often contend that individuals behave differently when others are observing their actions. Researchers Munger and Harris examined the behavior of individuals and found that when people know they are being watched, they are more likely to exhibit normal and socially acceptable behavior.[24] A 2012 study involving BWCs by Munger and Harris concluded that officers wearing BWCs had a 60 percent decrease in use-of-force incidents and an 88 percent decrease in the number of civilian complaints lodged against them.[25] The strategy behind BWCs is to reduce civilian complaints against police and officer use-of-force incidents against civilians, increase officer safety, and build stronger court cases.[26]

The overall benefits obtained from the use of BWCs have been advantageous to both law enforcement and citizens alike. BWCs have reduced civilian complaints against

---

[23] New York City Police Department, *Patrol Guide: Command Operations*, 212–123 (New York: NYPD, January 8, 2018), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/body-worn-cameras-patrol-guide.pdf.

[24] Kristen Munger and Shelby J. Harris, "Effects of an Observer on Handwashing in a Public Restroom," Perceptual and Motor Skills 69 (1989): 733–734, https://kmunger.files.wordpress.com/2007/09/munger-harris-1989-effects-of-an-observer-on-handwashing-in-a-public-restroom.pdf.

[25] Miller and Toliver, *Implementing a Body-Worn Camera Program*, 14.

[26] Paul Drover and Barak Ariel, "Leading an Experiment in Police Body-Worn Video Cameras," *International Criminal Justice Review* 25, no. 1 (March 1, 2015): 80–81, https://doi.org/10.1177/1057567715574374.

police officers, with sharp decreases in police use-of-force incidents and fewer falsified complaints made by citizens.[27] Internally, law enforcement organizations can use BWC footage to train and identify problematic tactics or officer behavior. BWC technology is also vital in reconstructing officer-involved shootings as well as documenting evidence, court testimony, and consents to search.

In addition to privacy concerns, questions remain as to when officers should be required to activate their BWCs. Policies vary by department, with some choosing to record every encounter and others allowing officer discretion of what and when to record. There are debatable positions by advocates and law enforcement alike on these issues. Officers from the Sunnyvale Police Department, who participated in a survey, show the negative impact BWCs have had on officer decision making. The survey found that "over half (14/23) strongly agreed or agreed with the statement, 'I feel like I have to follow the letter of the law when wearing my body-worn camera.'"[28] Furthermore, 15 officers indicated on the survey that they "felt uncomfortable 'cutting breaks' on the street."[29] Officers felt that discretion was more difficult when dealing with minor offenses. Officer interviews "suggested that a reason for this change is that cameras now made it possible for others, particularly superiors, to examine an officer's decision retrospectively and assess its appropriateness given the particular circumstances."[30] As one officer explained, "The possibility of increased scrutiny made him more likely to write a traffic ticket, instead of giving written warnings or just letting someone off with a 'pep-talk.'"[31] "More than half of the officers (13/24) reported that wearing a camera influenced how they communicated with people."[32] In fact, the officers acknowledged the potential for their words to extend beyond the individuals involved in an encounter: "Hence, they were more prone to exercise

---

[27] Miller and Toliver, *Implementing a Body-Worn Camera Program*, 5–7.

[28] Marthinus C. Koen, James J. Willis, and Stephen D. Mastrofski, "The Effects of Body-Worn Cameras on Police Organisation and Practice: A Theory-Based Analysis," *Policing and Society* (April 2018): 8, https://www.tandfonline.com/doi/pdf/10.1080/10439463.2018.1467907?needAccess=true.

[29] Koen, Willis, and Mastrofski, 8.

[30] Koen, Willis, and Mastrofski, 8.

[31] Koen, Willis, and Mastrofski, 8.

[32] Koen, Willis, and Mastrofski, 8.

'verbal caution,' which meant avoiding profanity, being mindful of the tone of their speech, and paying more attention to the content of what they said."[33]

Law enforcement technologies, specifically BWCs, can be ineffective without sound policies governing their use. The ACLU argues that BWCs "can be a win-win—but only if they are deployed within a framework of strong policies to ensure they protect the public without becoming yet another system for routine surveillance of the public and maintain public confidence in the integrity of those privacy protections. Without such a framework, their accountability benefits would not exceed their privacy risks."[34]

D. LITERATURE REVIEW

Law enforcement's use of surveillance technologies may create citizen fears of an "Orwellian society." Recent advances in technology become amplified, especially when combined with outpaced legislation drawing additional concerns that law enforcement agencies will have autonomy and misuse surveillance technologies. As such, in addition to privacy concerns, public trust challenges of law enforcement exist. This review examines the issues in two sections. The first section of this review provides an understanding of the legal and ethical dilemmas and the onus placed on law enforcement to balance privacy and security. The second section examines the literature related to public trust challenges faced by law enforcement.

1. Privacy versus Security

Privacy concerns specific to the use of law enforcement technologies can be traced back to the 1880s, when advancements in photography eased the use of equipment and enabled portable cameras for use outside photo studios. The portable camera then began to document the world in a new way and, as a result, created new privacy concerns.[35] An

---

[33] Koen, Willis, and Mastrofski, 12.

[34] Jay Stanley, *Police Body-Mounted Cameras: With Right Policies in Place, a Win for All*, version 2.0 (New York: American Civil Liberties Union, March 2015), 2, https://www.aclu.org/other/police-body-mounted-cameras-right-policies-place-win-all.

[35] Claudia Cuador, "From Street Photography to Face Recognition: Distinguishing between the Right to Be Seen and the Right to Be Recognized," *Nova Law Review* 41, no. 2 (2017): 5, https://nsuworks.nova.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=1998&context=nlr/.

evaluation of the literature of current frameworks, legal concerns, as well as law enforcement and government recommendations for real-time FRT provides a deeper understanding of the privacy challenges that the NYPD faces. The problem of how to mitigate individual privacy concerns remains unanswered. No universal policies exist, and therefore, no methods exist for data collection, sharing, and storage—raising ethical concerns of how law enforcement organizations will use FRT. A New York University study argues that law enforcement agencies should focus on ethical issues raised by sharing data because expanding the use of new technologies compromises the desire of individuals to have complete and absolute privacy.[36]

Critics express concern over big data, massive storage, and the analytic capabilities of new technologies. Ironically, citizens embrace certain technologies and fear others, even though they offer similar benefits and challenges. Technologies like FRT experience a combination of acceptance and rejection. For example, citizens laud FRT when used as a security feature on a smartphone or to create a talking emoji, but in the hands of law enforcement, that same technology creates negative feelings for many people. The reason behind the negative association of FRT use centers on the potential for diminished levels of privacy, which most citizens are accustomed to in a public setting. Privacy, as defined by Ruth Gavison, is "a measure of the access others have to you through information, attention, and physical proximity."[37] Gavison's definition contends that the lack of "privacy" evokes a negative connotation and anything that alters total privacy is a violation, an intrusion, or undesirable. Philosopher Jeffery Reiman provides a different definition of privacy: "The condition under which other people are deprived of access to either some information about you or some experience of you."[38] Another legal scholar, Anita Allen, contends that privacy has three dimensions: physical privacy, informational privacy, and proprietary privacy. Informational privacy is arguably the leading concern among citizens

---

[36] Julia Lane et al., *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge: Cambridge University Press, 2014), 49, https://www.nyu.edu/projects/nissenbaum/papers/BigDatasEndRun.pdf.

[37] Helen Fay Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Palo Alto, CA: Stanford University Press, 2010), 67.

[38] Nissenbaum, 70.

when law enforcement uses surveillance technologies due to the potential reduction of anonymity in public.

The public/private dichotomy infiltrates both legal and political discourse. The point of contention is that the definitions of public and private vary depending on the context. For example, the term private is associated with legal but personal engagements in intimate settings or with an expectation of privacy when using the internet. The public/private dichotomy also exists in government. In democratic societies, checks and balances establish strict guidelines for intrusions into citizen privacy. Citizens have an expectation of privacy, specifically when it involves government use of surveillance technologies to track them. Some view these checks and balances as the right to restrict the government access to personal records. Ironically, the U.S. Constitution does not explicitly define privacy.

According to a 1990 survey, 79 percent of Americans claim that if the Declaration of Independence was rewritten, they would be willing to add "privacy" in addition to "life, liberty, and the pursuit of happiness."[39] In another survey conducted in 2003, 95 percent of citizens reported a concern with the internet as well as how personal information is collected.[40] Actions, however, speak louder than words. Although many of the surveys identified serious privacy concerns over the use of personal information, surveys evaluating public benefits such as E-Z Pass, traceable search engines, discount shoppers' cards, and other modes of convenience were deemed favorable.[41] Also, only 20 percent of citizens claim to read privacy policies "most of the time," and even less (7 percent) complain about company privacy policies.[42]

Potential community concerns associated with the NYPD's use of real-time FRT are relevant to the discussion. Public mistrust of the police still exists, both with misuse of surveillance technologies and the methods by which law enforcement collects, shares, and

---

[39] Nissenbaum, 103.

[40] Nissenbaum, 103.

[41] Nissenbaum, 103.

[42] Nissenbaum, 103.

stores data. If the NYPD were to consider implementing real-time FRT, additional public trust challenges might arise. Law enforcement's deployment of real-time facial recognition may prompt citizen resistance. A recent analysis by Georgetown Law argues that although there are many benefits to FRT, significant risks remain to endanger individual privacy, civil liberties, and civil rights.[43] Critics argue that without regulation, law enforcement agencies would be free to collect and share information obtained from facial recognition databases without oversight. An analysis by the Center on Privacy and Technology at Georgetown Law argues that real-time FRT will create new paradigms in both policing and individual conceptualizations of the definition of freedom.[44]

Advocacy groups have resisted other law enforcement technologies, such as LPRs, which in the past have created animosity between citizens and the police. The ACLU argues that police organizations will use LPR technology as a tracking tool and that few guidelines exist to maintain the integrity of the system.[45] In addition, the ACLU cites specific cases where police officers misused LPR technology.[46] The vast majority of individuals with knowledge of LPR technology view it as an efficient, non-evasive crime-fighting tool. A report by RAND Corporation examines the benefits and challenges of LPR technology, noting the ACLU's belief that national use of LPR technology by law enforcement becomes a gateway for other technologies to infringe on constitutional

---

[43] Clare Garvie, Alvaro Bedoya, and Johnathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Washington, DC: Center on Privacy and Technology, Georgetown Law, October 18, 2016), 1, https://www.perpetuallineup.org.

[44] Garvie, Bedoya, and Frankle, 22.

[45] Catherine Crump, *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements* (New York: American Civil Liberties Union, July 2013), 2, https://www.aclu.org/issues/privacy-technology/location-tracking/you-are-being-tracked.

[46] Mariko Hirose, "Documents Uncover NYPD's Vast License Plate Reader Database," American Civil Liberties Union, January 25, 2016, https://www.aclu.org/blog/privacy-technology/location-tracking/documents-uncover-nypds-vast-license-plate-reader-database.

rights.[47] An opposing article suggests the ACLU has made several misleading statements about LPR technology, its use, and dissemination of collected data by law enforcement.[48]

Among advocacy groups, an overwhelming concern remains that the government is not willing to compromise security for privacy. Article 17 of the International Covenant on Civil and Political Rights declares, "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."[49] The House Committee on Oversight and Government reform oversaw a bipartisan hearing on March 22, 2017, to address law enforcement's use of FRT.[50] There was a strong emphasis on the policies created to mitigate privacy concerns. Both subcommittees identified numerous issues, but none of those have spurred the creation of new laws for facial recognition. While some political leaders and activist groups agree there is a need for legislation on FRT, they do not agree on how to accomplish a universal framework for law enforcement to follow.[51] The ACLU has provided recommendations to the National Telecommunications and Information Administration for an ethical framework for FRT, but specific legislation has yet to be created.[52]

---

[47] Keith Gierlack et al., *License Plate Readers for Law Enforcement: Opportunities and Obstacles* (Santa Monica, CA: RAND Corporation, 2014), 17–18, https://www.rand.org/pubs/research_reports/RR467.html.

[48] Joel Griffin, "LPR Technology Comes of Age," Security Info Watch, August 4, 2015, http://www.securityinfowatch.com/article/12099279/lpr-technology-comes-of-age.

[49] Francesca Bignami and Giorgio Resta, *Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance* (Rochester, NY: Social Science Research Network, 2018), 1, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3043771.

[50] *Hearing before the Committee to Review Law Enforcement's Policies on Facial Recognition Technology*, House, 115th Cong., 1st sess., March 22, 2017, https://oversight.house.gov/hearing/law-enforcements-use-facial-recognition-technology.

[51] John Byrne, "Emanuel Raises Facial Recognition Tech in Taxi vs. Ride-Share Debate," *Chicago Tribune*, November 7, 2017, http://www.chicagotribune.com/news/local/politics/ct-met-rahm-emanuel-rideshare-report-20171107-story.html.

[52] Catherine Crump, "An Ethical Framework for Face Recognition," American Civil Liberties Union, July 16, 2013, https://www.ntia.doc.gov/files/ntia/publications/aclu_an_ethical_framework_for_face_recognition.pdf.

The vast majority of literature on automatic or real-time FRT suggests that significant benefits exist for law enforcement agencies and corporations.[53] In addition, the literature explains that the use of real-time FRT by law enforcement has practical benefits because of recent technological developments.[54] The literature on the subject suggests that data collection from FRT has favorable results when used in the field by law enforcement and on the battlefield by the U.S. military.[55] Federal law enforcement agencies collectively agree that transparency needs to exist between law enforcement and citizens when it involves how law enforcement organizations collect and use biometric information.[56] The Department of Homeland Security (DHS) took several steps to create policies and procedures for biometric technologies that have strict standard operating procedures. DHS uses the Automated Biometric Identification System for storing and processing biometric information.[57] Privacy impact assessments provide citizens with detailed information on how federal law enforcement collects, shares, and uses biometric information.[58]

Some of the literature examines the success of real-time FRT in companies such as Facebook and JetBlue.[59] Concerns still exist, however, in such areas as performance,

---

[53] Future of Privacy Forum, *Privacy Principles for Facial Recognition Technology* (Washington, DC: Future of Privacy Forum, December 2015), https://fpf.org/wp-content/uploads/2015/12/Dec9Working-Paper-FacialRecognitionPrivacyPrinciples-For-Web.pdf.

[54] Jeerawat Detsing and Mahasak Ketcham, "Detection and Facial Recognition for Investigation," in *International Conference on Digital Arts, Media and Technology* (Piscataway, NJ: IEEE, 2017), 407–409, https://doi.org/10.1109/ICDAMT.2017.7905002.

[55] Glenn J. Voelz, *Rise of iWar: Identity, Information, and the Individualization of Modern Warfare* (New York: Skyhorse Publishing, 2018), 1–3, 10, https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1292

[56] Kimberly J. Del Greco, "Law Enforcement's Use of Facial Recognition Technology," Federal Bureau of Investigations, March 22, 2017, https://www.fbi.gov/news/testimony/law-enforcements-use-of-facial-recognition-technology.

[57] "Privacy Impact Assessment for the Automated Biometric Identification System (IDENT)," Department of Homeland Security, accessed August 8, 2018, 2–4, https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-identappendices-august2017.pdf; and W. Jeberson and Lucky Sharma, "Survey on Big Data for Counter Terrorism," *International Journal of Innovations and Advancement in Computer Science* 4 (May 2015).

[58] Department of Homeland Security, 5.

[59] Wendy Davis, "Facial Recognition Technology Nab Criminals-and Raises Privacy Concerns," ABA Journal, October 2017, http://www.abajournal.com/magazine/article/facial_recognition_technology_crime_ privacy.

intentional circumvention, and overall accuracy, but some are beginning to accept the presence of FRT as part of everyday life.[60] A December 2017 report by the Center on Privacy and Technology at Georgetown Law argues strongly against using FRT to identify passengers. The report suggests, "DHS should justify its investment in face scans by supplying evidence of the problem it purportedly solves."[61] Furthermore, DHS needs to conduct a cost analysis of the capabilities of the FRT air exit system to determine whether it is beneficial and requires additional funding or it should be disbanded and release finances to other initiatives.[62]

The Constitution Project, a bipartisan committee, is attempting to lobby for strong laws to protect citizens from the pervasive use of facial recognition. Jake Laperruque, senior counsel at the Constitution Project, claims that facial recognition is an invasive technology, and, if no laws exist, law enforcement agencies can and probably will abuse it.[63] A report by the Constitution Project acknowledges that real-time facial recognition can scan faces all day without limitations and without depleting police resources.[64] The upshot, however, is that any individual can be scanned and possibly tracked by law enforcement at events, demonstrations, political rallies, or protests—likely without any legal authority.[65]

Both advocacy groups and law enforcement desire a framework for how FRT, particularly real-time facial recognition, should be implemented to ensure that law

---

[60] Koichi Ito and Takafumi Aoki, "Recent Advances in Biometric Recognition," *ITE Transactions on Media Technology and Applications* 6, no. 1 (2018): 64–65, https://doi.org/10.3169/mta.6.64.

[61] Laura M. Moy, Harrison Rudolph, and Alvaro M. Bedoya, *Not Ready for Takeoff: Face Scans at Airport Departure Gates* (Washington, DC: Center on Privacy and Technology, Georgetown Law, December 21, 2017), 3–4, https://www.airportfacescans.com/sites/default/files/Biometrics_Report__Not_Ready_For_Takeoff.pdf.

[62] Moy, Rudolph, and Bedoya, 5.

[63] Jake Laperruque, "Preserving the Right to Obscurity in the Age of Facial Recognition," Century Foundation, October 20, 2017, https://tcf.org/content/report/preserving-right-obscurity-age-facial-recognition/.

[64] "Law Enforcement Facial Recognition Is a Powerful Surveillance Technology in Need of Independent Checks and Limits," Constitution Project, March 30, 2017, 1–2, https://constitutionproject.org/wp-content/uploads/2017/03/Facial-Recognition-Statement-for-Record_The-Constitution-Project.pdf.

[65] Constitution Project, 3.

enforcement officers do not infringe on individual constitutional rights. MIT researcher Joy Buolamwini argues that FRT already infringes on constitutional rights because flaws in facial recognition algorithms result in a predetermined bias—by design—that identifies a person.[66] Problematically, under current law, any police organization can access and disseminate facial recognition information on law-abiding individuals. In a 2016 article, Laura Sydell notes that the Federal Bureau of Investigation (FBI)'s facial recognition database includes driver's license photos from 16 different states.[67] A general concern is that this and similar databases will continue to grow and be shared with federal, state, and local law enforcement agencies.

The FBI believes that law enforcement should move forward with some form of "automated" FRT, with its analysis appearing to be in stark contrast to Sydell's findings, along with the findings of others.[68] FBI documents were the only sources in the literature that focused on adversarial threats as the top priority—whereas other authors concentrated their analyses on identifying privacy concerns. Although very little scholarly literature exists on real-time facial recognition for use by law enforcement in urban subway systems, there is, however, a recent article by Noah McClain that examines surveillance technologies in the New York City subway system. He argues the importance of "looking beyond the claims of technical efficacy in the study of security and surveillance to discover how technologies of inspection and control work, as a means to cut through the heavy rhetorical packaging in which they are sold to their publics."[69] McClain's position forecasts the belief that FRT has arrived, whether the public approves of its use or not.

---

[66] Michael Skirpan and Tom Yeh, "Designing a Moral Compass for the Future of Computer Vision using Speculative Analysis," in 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (Piscataway, NJ: IEEE, 2017), 64, http://openaccess.thecvf.com/content_cvpr_2017_workshops/w16/papers/Yeh_Designing_a_Moral_CVPR_2017_paper.pdf.

[67] Laura Sydell, "It Ain't Me, Babe: Researchers Find Flaws in Police Facial Recognition Technology," NPR, October 25, 2016, http://www.npr.org/sections/alltechconsidered/2016/10/25/499176469/it-aint-me-babe-researchers-find-flaws-in-police-facial-recognition.

[68] Del Greco, "Law Enforcement's Use of Facial Recognition."

[69] Noah McClain, "The Horizons of Technological Control: Automated Surveillance in the New York Subway," Information, Communication & Society 21, no. 1 (2018): 46, https://doi.org/10.1080/1369118X.2016.1260624.

A delicate balance exists between the citizens' desire for privacy and their need for security. These concerns often shift on a pendulum, swaying back and forth based on national and global events. Such questions as "Is it even possible to maintain privacy in an age where our daily actions can be monitored?" are reasonable and directly correlate with advancements in technology and new social media platforms.[70] FRT has a place in the natural progression of technological tools—from the installation of police call boxes in 1877, to fingerprint analysis, to CCTV cameras, and finally to more modern law enforcement technologies such as BWCs and drones.

2. Transparency

The foundation of policing is based on collaboration with citizens, public support, police transparency, and citizen acceptance of policing strategies, tactics, and policies. Lewis, Daniel, and Kalalea contend that in every police–citizen interaction, police earn a new friend or a new enemy.[71] This reality illustrates the dire need for police officers to create as many positive interactions as possible with citizens. Historically, efforts have been made to involve the community in policing. Most researchers contend that community policing encompasses three main ideas:

> 1) collaborative partnerships between the community and the police, while collectively address and prioritize community concerns; 2) organizational transformation, through which management and personnel develop the structure to collaborate with the community effectively; and 3) problem solving through "proactive and systematic examination of identified problems to develop and evaluate effective responses."[72]

---

[70] Susan McCoy, "O' Big Brother Where Art Thou?: The Constitutional Use of Facial-Recognition Technology," *John Marshall Journal of Computer & Information Law* 20, no. 3 (Spring 2002): 471.

[71] Stephanie Daniel, Nicole Lewis, and Kalalea Kalalea, "In the Wake of Broken Windows Policing How Aggressive Policing Contributed to East Harlem Residents Distrust of Police" (master's capstone, City University of New York, 2016), 2.

[72] Kathleen O'Reilly, "Transparency, Accountability, and Engagement: A Recipe for Building Trust in Policing" (master's thesis, Naval Postgraduate School, June 2017), 11.

In the NYPD, the first community policing strategy began in 1984 as a pilot program in the 72nd Precinct.[73] The NYPD rolled out the community patrol officer program (CPOP) during an era when significant mistrust of the police existed. The NYPD designed a strategy to combat community mistrust, instructing the community policing officer to foster relationships with community members and to solve the issues of the community collectively. The program, however, never gained acceptance from within the NYPD. One researcher acknowledges that other officers identified community police officers as "privileged social workers, detached from the department's daily crime-fighting pressures."[74] It was not until 2014, because of increased citizen concern, that the NYPD looked to formulate a new plan to address citizen mistrust.

Citizens, legislators, and members of the media have scrutinized several recent fatal police-involved use-of-force incidents. Former Secretary of State Hillary Clinton stated during the 2016 presidential election, "The deaths of Alton and Philando drove home how urgently we need to make reforms to policing and criminal justice . . . how we cannot rest until we root out implicit bias and stop the killings of African-Americans."[75] Clinton eluded to separate incidents—the deaths of Alton Sterling and Philando Castile, who were both shot and killed by police. Demonstrations, protests, and violence against the police, including several assassinations of police officers, occurred around the country as retribution for vigorously contested police-involved fatal use-of-force incidents.

The recent formation of new civil rights groups—Black Lives Matter, the Anti-Police Terror Project, and Communities United for Police Reform (CUFPR) among others—illustrates a growing citizen response to mistrust of law enforcement. CUFPR has created a brochure to inform citizens of their rights following an interaction with the

---

[73] Eli B. Silverman, *NYPD Battles Crime: Innovative Strategies in Policing* (Boston: Northeastern University Press, 1999), 55.

[74] Silverman, 56.

[75] "Full Transcript of Hillary Clinton's NAACP Speech: 'This Madness Has to Stop,'" *Fortune*, July 18, 2016, http://fortune.com/2016/07/18/hillary-clinton-speech-naacp-transcript/.

police.[76] The brochure reminds citizens, "Police officers can be unpredictable and can quickly escalate a situation, particularly if they feel unsafe, disrespected, or that they don't have control of the situation."[77] The brochure's message depicts inimical relations and mistrust of police by citizens; it also illuminates the misnomers that reflect unintentional misunderstandings and implicit bias of both police and citizens. Recent literature on police relations with citizens focuses less on law enforcement technologies and more on police use-of-force, implicit bias by police officers, and the need for transparency from law enforcement.

In 2014, one of the priorities of the newly appointed Mayor of New York City, Bill de Blasio, was to bridge the existing gap between citizens and the NYPD. Mayor de Blasio immediately appointed William J. Bratton to lead the NYPD, and his role was clear: continue to reduce crime and cultivate relationships between the police and the communities they serve. Bratton's appointment was his second tenure as police commissioner of New York City—he was already familiar with its dynamics and challenges. Bratton brought with him decades of police leadership from when he left the NYPD in 1996, but by 2014, new challenges had emerged, particularly with damaged relations between communities and the NYPD. In previous years, the NYPD's stop, question, and frisk (SQF) policy resulted in criticism nationwide and eventual federal monitoring after several lawsuits involving unlawful stops. Deficiencies in both policy and officer discretion caused critics to label "stop and frisk" a biased practice.[78] Statistical SQF data and citizen perception accentuated the fact that the existing practice needed an evaluation. In 2011, there were 685,724 persons stopped, and the stop did not result in an arrest 88 percent of the time.[79] In 2013, a legislative decision by Judge Analisa Torres

---

[76] "Know Your Rights! Help End Discriminatory, Abusive & Illegal Policing!" Communities United for Police Reform, accessed May 6, 2018, http://changethenypd.org/resources/know-your-rights-help-end-discriminatory-abusive-illegal-policing.

[77] Communities United for Police Reform.

[78] Michael D. White and Henry F. Fradella, *Stop and Frisk: The Use and Abuse of a Controversial Policing Tactic* (New York University Press, 2016), 7.

[79] Al Baker, "Street Stops by New York City Police Have Plummeted," *New York Times*, May 30, 2017, https://www.nytimes.com/2017/05/30/nyregion/nypd-stop-and-frisk.html.

ruled the practice of SQF as unconstitutional.[80] Federal Judge Shira A. Scheindlin appointed independent monitor Peter L. Zimroth to oversee changes in the SQF strategy. In 2017, there were 11,553 people questioned under the practice. Zimroth stated, "Things are trending in the right direction" with fewer stops on record than in prior years.[81] Even with fewer stops of individuals, violent crimes continue to decline in New York City. In 2017, there were 292 homicides, the lowest on record since 1951 (243).[82] Recent crime reductions can be contributed to improved transparency within the NYPD and the implementation of neighborhood policing.

Neighborhood policing is an innovative strategy, dubbed a new way of policing, developed by the NYPD to rebuild trust between the community and police. Neighborhood policing does not derive from CPOP because its foundational principles and objectives are different. Neighborhood coordination officers help rebuild trust and get to know the people in the community. Moving forward, the NYPD has created a new strategy to rebrand its image. In 2018, a new department initiative, called "Build the Block," became part of the neighborhood-policing model.

The strategy behind neighborhood policing is to facilitate collaboration among members of the community to share the responsibility of safety in New York City neighborhoods, allowing communities to work in partnership with the NYPD. Build the Block neighborhood safety meetings "are strategy sessions between local police officers and the public they serve. These meetings have two simple goals: identify the public safety challenges of a specific neighborhood and discuss potential solutions."[83] Transparency and trust between community members and police are essential parts of the crime-fighting mission. Initiating new strategies, technologies, or policies, increases the NYPD's chances

---

[80] Baker.

[81] J. David Goodman, "Court-Appointed Police Monitor Has Fought for City and against It," *New York Times*, August 13, 2013, https://www.nytimes.com/2013/08/14/nyregion/court-appointed-police-monitor-has-fought-for-city-and-against-it.html.

[82] "Crime Statistics," New York City Police Department, accessed July 17, 2018, https://www1.nyc.gov/site/nypd/stats/crime-statistics/crime-statistics-landing.page.

[83] "Build the Block," New York City Police Department, accessed July 17, 2018, https://www1.nyc.gov/site/nypd/bureaus/patrol/buildtheblock.page.

for overall success and of public acceptance because citizens feel involved and express their concerns to the department.

E. RESEARCH DESIGN

This thesis uses the comparative case study method to examine the benefits and challenges of LPR technology to address how the NYPD can mitigate concerns and evaluate real-time FRT for use in the New York City subway system. The comparison examines the NYPD's use of LPR technology and then identifies each of the benefits and challenges. The benefits were identified through the literature, public discourse, case law, internal open-source NYPD documents, and studies from scholars and advocacy groups. The research addresses the extent to which LPRs are analogous to FRT and how the use of LPRs can provide the NYPD with a roadmap for public support of real-time FRT. The possible vulnerabilities of real-time FRT may include reduced levels of citizen privacy, public trust challenges, and overall unreliability. The benefits of LPR technology and FRT examined in this thesis are divided into two categories. The first category illustrates the crime prevention benefits of LPRs and FRT, and the second identifies law enforcement and public benefits. The order of each categorical benefit begins with the most significant use for each technology.

This thesis asserts that the NYPD does not have to start from scratch to figure out how to mitigate the challenges to reap public benefits of real-time FRT. The NYPD and other law enforcement organizations already use such surveillance technologies as LPRs, which scan license plates to ascertain pertinent information about vehicles and their registered owners. Many of the challenges associated with LPRs have already been mitigated, resulting in citizen acceptance and expanded use. The public benefit and overall citizen acceptance of LPR technology can provide a framework for the NYPD to implement real-time FRT.

Advancements in FRT have created significant benefits for law enforcement organizations to reduce crime and potentially mitigate acts of terrorism. Although significant benefits exist, the NYPD faces challenges that require a thorough evaluation before implementing real-time FRT for use in the New York City subway system. The

NYPD, however, can leverage lessons learned from LPR technology. Both LPR technology and FRT are similar in that they share many of the same benefits and challenges. Documents show that more law enforcement agencies in the United States are implementing LPR technology. The NYPD uses LPRs, and recent technology advancements have created additional benefits. Although several new benefits have been identified, new challenges have emerged. The NYPD may need to re-evaluate privacy, accuracy, and public trust concerns with LPR technology.

F. CHAPTER OUTLINE

An overview of LPRs, their use in law enforcement, and the identified benefits and challenges of the technology are presented in Chapter II. Law enforcement use of FRT has negative perceptions, and critics of the technology are quick to document concerns that are unintentionally analogous to the concerns of LPRs. Chapter III provides an overview of FRT, its current and projected use by law enforcement, and an examination of the technology's benefits and challenges. Chapter IV illustrates the ability for decision-makers to mitigate the challenges of law enforcement's use of real-time FRT. With public support, the NYPD can effectively implement real-time FRT in the New York City subway system. The chapter then concludes with the lessons learned from LPRs and FRT and provides recommendations to the NYPD for next steps and further research.

II. LICENSE PLATE READERS

Communities benefit from LPR technology despite privacy concerns and the contention of critics—such as the ACLU, which argues that law enforcement agencies should not be able to collect and store information on law-abiding citizens not suspected of any criminal wrongdoing.[84] This chapter provides an overview of LPR technology, including its definition and history as well as the benefits of LPR technology for law enforcement and the public. It then examines the challenges of LPR. This chapter shows that the benefits of LPR technology outweigh its challenges. The benefits and challenges of LPR technology in this chapter provide a framework to analyze the benefits and challenges of real-time FRT.

A. OVERVIEW

This section explains how LPR technology was developed, how it was first used, and how it is used today. Then, it explains how officers use LPR technology, provides the NYPD's definition of LPR technology, and describes how LPRs supplement police operations.

1. History of License Plate Reader Technology

In 1976, the Police Scientific Development Branch of the Home Office in the United Kingdom invented LPR technology, also known as automatic number plate recognition, which captured the image of a license plate and attempted to match it against a pre-determined hot-list containing reported information on stolen vehicles.[85] Initially, LPRs were developed to assist law enforcement in identifying stolen vehicles, but in April 1993, terrorists detonated a bomb inside a truck in the financial area of London. Following

---

[84] Ben Eisler, "ACLU Concerned Automatic License Plate Readers May Invade Privacy," WJLA News, July 30 2012, http://wjla.com/news/local/aclu-concerned-red-light-cameras-may-invade-privacy-78301.

[85] David J. Roberts and Meghann Casanova, *Automated License Plate Recognition Use by Law Enforcement: Policy and Operational Guide, Summary*, doc. 239605 (Alexandria, VA: International Association of Chiefs of Police, September 2012), 3, https://www.ncjrs.gov/pdffiles1/nij/grants/239605.pdf.

the attack, City of London Police included LPRs in its new strategy to secure London, known today as the "ring of steel."[86] The goal of the City of London Police was to apply combat-style strategies in civilian settings to protect citizens, or "fortress urbanism."[87] LPR technology gave police valuable intelligence by identifying every vehicle that entered London—which was necessary because the Irish Republican Army had identified central London as an ideal location to conduct bombings.[88] As acts of terrorism continued in the 1990s, the use of LPR technology expanded with little citizen resistance. In 1997, LPR cameras were placed at the entrances of the ring of steel. In 2002, the use of LPRs expanded to nine different police agencies.[89] In 2003, LPRs were used to facilitate traffic congestion tolls, and in 2006, the data storage capabilities were enhanced for a capacity of 50 million plate scans per day.[90]

In 2008, the NYPD launched a similar strategy to strengthen resiliency capabilities by using technology, increased police presence, and collaboration with the private sector to protect lower Manhattan and sensitive locations, such as the Stock Exchange, the World Trade Center, and Federal Plaza. This strategy, known as the Lower Manhattan Security Initiative (LMSI), uses both mobile and stationary LPR cameras, uniformed police presence, and technology to detect threats and conduct "pre-operational terrorist surveillance," which augments the deployment of specially trained police officers and integrated technology platforms.[91] Since 2008, the LMSI has expanded, involving the better integration of technologies such as radiation pagers, LPR technology, and CCTV cameras. The success of the LMSI has warranted further expansion into other areas of

---

[86] J. Mullins, "Ring of Steel II: New York City Gets Set to Replicate London's High-Security Zone," *IEEE Spectrum* 43, no. 7 (July 2006): 12, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1652996.

[87] "Ring of Steel," MAS Context, June 25, 2014, http://www.mascontext.com/issues/22-surveillance-summer-14/ring-of-steel/.

[88] MAS Context.

[89] "Protection of Freedoms Bill," UK Parliament, accessed August 8, 2008, https://publications.parliament.uk/pa/cm201011/cmpublic/protection/memo/pf11.htm.

[90] UK Parliament.

[91] "Counterterrorism," New York City Police Department, accessed May 14, 2018, https://www1.nyc.gov/site/nypd/bureaus/investigative/counterterrorism.page.

Manhattan.[92] In addition to the NYPD, 71 percent of law enforcement agencies in the United States were using LPR technology as of 2012.[93] Five years later, in 2017, researchers projected that approximately 85 percent of police agencies would obtain funding to purchase LPR equipment.[94]

In 2013, the NYPD expanded the use of LPR readers throughout New York City.[95] Citing that no laws prevent the use of surveillance technology to prevent crime, the NYPD expanded LPR use and leveraged its ability to perform additional functions. For example, in addition to identifying stolen vehicles, the NYPD often examines LPR data to assist in police investigations. Officers are instantly able to recover a stolen vehicle based on real-time information supplied to an officer on patrol. Furthermore, detectives can leverage LPR data to piece together on-going investigations. With new advancements in LPR technology, local governments, law enforcement, and private companies all leverage LPRs to perform various tasks—real-time traffic monitoring, toll collections, parking-lot access control, and traffic enforcement—not to mention cameras to enforce traffic laws.[96]

Since 2016, the public has accepted the NYPD's use of LPR technology due to tangible public benefits. An example of such benefits occurred in June 2018, when a teenage boy was attacked on a Bronx street corner by several perpetrators. In a case of mistaken identity, gang members stabbed the boy to death, but his murder was captured on surveillance cameras and cell phone videos. When the videos were posted on social media, his horrific and untimely death created outrage among both citizens and law enforcement.

---

[92] New York City Police Department, "Midtown Manhattan Security Initiative" (press release, NYPD, September 20, 2010), http://www.nyc.gov/html/nypd/html/pr/pr_2010_midtown_security_initiative.shtml.

[93] Chuck Wexler, "Introduction," in *How are Innovations in Technology Transforming Policing* (Washington, DC: Police Executive Research Forum, January 2012), iii, http://www.policeforum.org/assets/docs/Critical_Issues_Series/how%20are%20innovations%20in%20technology%20transforming%20policing%202012.pdf.

[94] Gierlack et al., *License Plate Readers for Law Enforcement*, 8.

[95] Chris Francescani, "NYPD Expands Surveillance Net to Fight Crime as well as Terrorism," Reuters, June 21, 2013, https://www.reuters.com/article/usa-ny-surveillance/nypd-expands-surveillance-net-to-fight-crime-as-well-as-terrorism-idUSL2N0EV0D220130621.

[96] Shan Du et al., "Automatic License Plate Recognition: A State-of-the-Art Review," *IEEE Transactions on Circuits and Systems for Video Technology* 23, no. 2 (February 2013): 311–312, https://doi.org/10.1109/TCSVT.2012.2203741.

Numerous gang members had been involved and were considered an extreme risk to citizen safety. After an extensive investigation, NYPD detectives arrested most of the perpetrators within a few days. An LPR caught the last remaining suspect on the loose along Interstate 84 in Danbury, Connecticut.[97] High-profile cases in which dangerous perpetrators are apprehended because of LPRs demonstrate the technology's benefit to the safety of citizens.

2. How License Plate Readers Work

LPR technology operates using high-speed infrared cameras that first photograph license plates, then create an image of the plate, and match the image to a law enforcement hot-list, which can compare the scanned image with local, state, and federal databases. The NYPD clearly defines an LPR and in its policy requires that an LPR operator verify information received from a device before taking police action:

> An LPR device can identify a target plate within seconds. LPR devices may read each license plate passed and alert the LPR operator when there is a match to a list of specific or partial license plate numbers. The LPR device is not automatically connected to NYSPIN [the New York State Police Identification Network], is not programmed to scan the state of registration on a license plate and will activate upon a partial scan match. Therefore, it is absolutely essential that the LPR operator verify the current status of a vehicle through NYSPIN prior to initiating any law enforcement action (e.g., arrest, summons, etc.).[98]

The verification of LPR information assists the officer in determining whether to conduct a known-risk vehicle stop (KRVS), a traffic stop that potentially has increased risks for the police officers initiating it. An officer conducting a KRVS must exercise additional tactical considerations and make a more cautious approach, based on the potential threat identified by the LPR. Figure 1 illustrates how law enforcement uses LPR technology.

---

[97] Jim Shay, "License Plate Reader Help Nab Suspect in Slaying of NYPD Explorer," Officer, July 11, 2018, https://www.officer.com/command-hq/technology/traffic/lpr-license-plate-recognition/news/21012850/license-plate-reader-help-nab-suspect-in-slaying-of-nypd-explorer-lesandro-junior-guzmanfeliz.

[98] New York City Police Department, *Patrol Guide: "Padlock Law" Program*, 291–31 (New York: NYPD, July 1, 2014), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/public-pguide3.pdf.

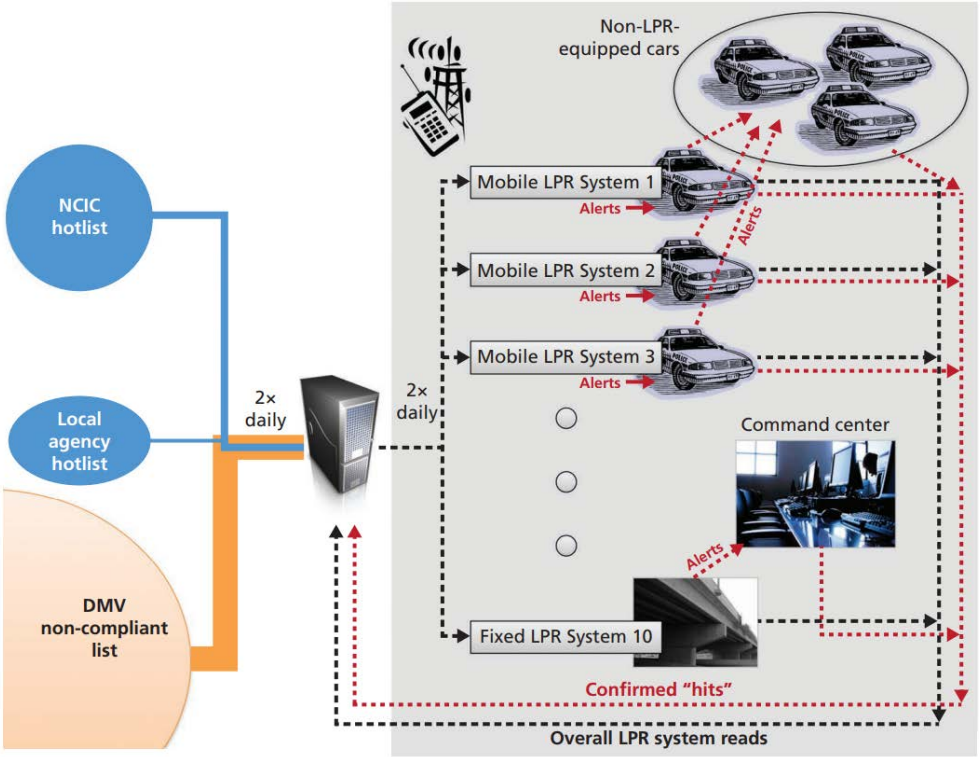

Figure 1. Notional Large-Scale, Integrated Departmental LPR Setup[99]

It would be impossible for officers to conduct license plate checks at the same rate as an LPR reader, which can analyze up to 1,800 license plates per minute. Each LPR device costs between $10,000 and $22,000, depending on the manufacturer and the type—vehicle-equipped, portable, or fixed.[100] Despite the cost, differing LPR deployments allow law enforcement to apply various crime-fighting or tactical strategies. For example, LPRs installed at fixed locations, such as bridges and tunnels, provide law enforcement specific information regarding individual vehicle whereabouts and the ability to identify all vehicles entering and exiting specific locations within New York City. The LPR cameras installed on patrol vehicles can create a record of license plates near a crime scene, which may yield valuable evidence in future criminal proceedings. For example, law enforcement officers can examine LPR data near a crime scene and use them to supplement other pieces of

[99] Source: Gierlack et al., *License Plate Readers for Law Enforcement*, 65.

[100] Roberts and Casanova, *Automated License Plate Recognition*, 2.

evidence to identify potential suspects or witnesses. Portable LPR cameras provide law enforcement agencies the versatility to record license plate data in locations where fixed LPR cameras do not exist, but the surveillance needs—at massive demonstrations, parades, or events—may be necessary.

B. BENEFITS OF LPR TECHNOLOGY

Due to recent improvements, law enforcement agencies have been researching new ways to use LPR technology, expanding its uses exponentially from its original purpose to identify stolen vehicles. Over the last 22 years, the number of stolen vehicles has drastically decreased, and although no specific evidence connects the decline to LPR technology, such a trend implies a nexus between technology and efficiencies in policing. As a matter of course, other law enforcement strategies and technologies, including better vehicle security features and GPS systems, have also aided this trend in terms of prevention. Nonetheless, cars are still stolen as thieves adapt to theft deterrence technologies, which suggest a continued need for LPR technology. In 1996, nearly 1.4 million vehicles were reported stolen in the United States while, in 2015, only 723,186 vehicles were stolen—a 53 percent decrease, despite an increase of 56,190,248 people and 58 million more registered vehicles nationwide.[101] While identifying or tracking stolen vehicles remains the primary use of LPRs in law enforcement, other public safety benefits exist. LPRs can assist in decreasing crime, potentially prevent and help investigate acts of terrorism, identify wanted persons, assist in detective investigations, provide additional officer safety, support individuals with mental health needs, locate missing persons, and be used in conjunction with other law enforcement technologies such as facial recognition.

1. Crime Prevention Benefits

The most important benefits of LPRs all involve preventing or reducing crime. The use of LPRs has tangible benefits in reducing and investigating crimes.

---

[101] "2015 Crime in the United States," Federal Bureau of Investigation, accessed June 3, 2018, https://ucr.fbi.gov/crime-in-the-u.s/2015/crime-in-the-u.s.-2015/tables/table-1; and "Number of Motor Vehicles Registered in the United States from 1990 to 2016 (in 1,000s)," Statista, accessed June 3, 2018, https://www.statista.com/statistics/183505/number-of-vehicles-in-the-united-states-since-1990/.

a. Preventing Violent Crime

With a comprehensive policy and crime reduction strategy in place, in addition to recovering stolen vehicles, LPRs can assist police departments in reducing violent crimes such as homicide, rape, robbery, and felony assault. In 2004, the Ohio State Highway Patrol conducted a four-month test of LPR technology to determine its effectiveness in crime fighting. Officers made 23 arrests and recovered 24 stolen vehicles.[102] Since the implementation of LPR technology by the Rockford, Illinois, Police Department, there has been an 8 percent reduction in violent crime, and property crime has decreased by 5 percent.[103] Koper, Taylor, and Woods contend in a 2013 study that LPR technology could be an effective tool in reducing crime in targeted areas.[104] By analyzing crime data, officers can deploy LPRs in specific locations with increases in crime to identify and arrest operators of stolen vehicles and investigate vehicles of past violent crimes—such as robberies and assaults—to identify potential patterns. In addition, law enforcement officers can use LPRs to investigate non-violent crimes, such as thefts from vehicles, to identify similarities in specific areas.

b. Investigating Terrorism

LPR technology can be used to help investigate and may prevent terror attacks. Terrorists are increasing their use of vehicles to conduct vehicle-ramming attacks (VRAs) against innocent pedestrians. More than a dozen VRAs have occurred around the world since 2014, claiming the lives of more than 170 people.[105] The NYPD used LPRs to investigate a recent VRA in lower Manhattan. On October 31, 2017, Sayfullo Saipov drove

---

[102] Tim Dees, "Finding Stolen Vehicles," Hendon Media Group, accessed June 3, 2018, http://www.hendonpub.com/resources/article_archive/results/details?id=3901.

[103] Jeff Kolkey, "How One Illinois City Uses Automatic License Plate Readers and Other Police Tech," Government Technology, May 21, 2018, http://www.govtech.com/dc/How-One-Illinois-City-Uses-Automatic-License-Plate-Readers-and-Other-Police-Tech.html.

[104] Christopher S. Koper, Bruce G. Taylor, and Daniel J. Woods, "A Randomized Test of Initial and Residual Deterrence from Directed Patrols and Use of License Plate Readers at Crime Hot Spots," *Journal of Experimental Criminology* 9, no. 2 (June 2013): 217, 213–244, https://www.voiceofsandiego.org/wp-content/uploads/2018/04/Koper-et-al-2.pdf.

[105] "Vehicles as Weapons of Terror," Counter Extremism Project, May 22, 2017, https://www.counterextremism.com/vehicles-as-weapons-of-terror.

a truck onto a pedestrian jogging path in lower Manhattan for approximately one mile, killing eight people and injuring 11.[106] Responding officers shot and wounded Saipov before placing him under arrest. Crime scene investigators recovered documents inside the truck, which contained an Islamic State flag and documentation of his radicalization.

According to John Miller, NYPD deputy commissioner of counterterrorism and intelligence, LPR data tracked Saipov's movements leading up to the attack. When examined, his movements offered additional investigative value. Detectives were able to track Saipov's movements throughout the City and combine video footage from CCTV cameras along his traveled route. In addition, detectives analyzed LPR data to identify potential accomplices and examine Saipov's four prior trips into Manhattan. Furthermore, the NYPD maintains close relationships with members of various truck rental businesses to prevent VRAs or truck bombing attacks. Starting in 2016, the NYPD began visiting truck-rental companies and discussed suspicious indicators and methods to report suspicious activity. Any rented vehicle that is later deemed suspicious, based on an investigation by law enforcement, can be entered into an LPR database and stopped by law enforcement, which may mitigate a future attack.

The NYPD does not release the specific number of LPR cameras in New York City, but current cameras do provide near-instant information that can be accessed using the department's domain awareness system (DAS), which links department databases into one searchable application. LPR data was an essential part of the analysis to retrace the aforementioned attack in New York City. Also, law enforcement can use data obtained from LPRs to produce valuable information for future movements of potential terrorists moving through the streets of New York City, which may shed some insight into future target selection. In investigating the 2017 VRA, LPR data enabled the NYPD to reconstruct a timeline of the events that preceded the attack. In addition, as LPR use by different law enforcement agencies expands, traditional and new uses will benefit law enforcement crime-fighting and counter-terrorism strategies.

---

[106] Corey Kilgannon and Joseph Goldstein, "Sayfullo Saipov, the Suspect in the New York Terror Attack, and His Past," *New York Times*, November 1, 2017, https://www.nytimes.com/2017/10/31/nyregion/sayfullo-saipov-manhattan-truck-attack.html.

c. Real-Time Identification of Wanted Persons and Known Suspects

LPR real-time data, obtained from mobile, stationary, and portable readers, can provide license plate information that may become valuable in other active criminal investigations.[107] Larger police departments, such as the NYPD, have numerous LPR cameras in mobile and fixed positions throughout their cities. Law enforcement can, as needed, search the captured real-time data for valuable investigatory information. For example, when television news reporter Vester Lee Flanagan was murdered in Virginia on live television, law enforcement relied on real-time LPR data to apprehend his former colleague for the crime.[108] Law enforcement officers added the suspect's plate number to the police hot-list, which led to his arrest.

d. Investigative Assistance

NYPD software has the ability to perform data integration, combining information—complaint reports, summons activity, arrest activity, 3–1-1 and 9–1-1 calls, wanted persons, police department vehicle locations, LPR data, and other information—to portray a detailed snapshot of the current environment in New York City. The NYPD uses its DAS to capture and create a tactical response based on real-time data. As a result, the NYPD can swiftly make accurate assessments of a vehicle's present and past locations, as well as other metrics, in real time.[109]

This saturation of data can be useful in a variety of ways. For example, following a comprehensive criminal investigation, detectives used LPR technology to obtain probable cause in the arrest of Marat G. Mikhaylich for a string of nine bank robberies.[110] Mikhaylich managed to elude capture, but after robbing a bank in Edison, New Jersey, he

---

[107] Laura J. Moriarty, ed., *Criminal Justice Technology in the 21st Century*, 3rd ed. (Springfield, IL: Charles C. Thomas Publisher, 2017), 263. Smaller law enforcement organizations, however, may be limited in effectiveness due to a lack of real-time data, mainly because of the insufficient number of LPRs.

[108] Nathan Tempey, "The NYPD Is Tracking Drivers across the Country Using License Plate Readers," Gothamist, January 26, 2016, http://gothamist.com/2016/01/26/license_plate_readers_nypd.php.

[109] Jeberson and Sharma, "Survey on Big Data," 202.

[110] Al Baker, "License Plate Cameras Aid in Police Investigations," *New York Times*, April 11, 2011, https://www.nytimes.com/2011/04/12/nyregion/12plates.html.

stole a livery cab and drove to Queens, New York. LPR scans identified the stolen cab, and when detectives located it the next morning, they were able to arrest Mikhaylich inside the same vehicle.[111] His arrest was the result of the LPR technology's ability to analyze historical LPR data. Without it, Mikhaylich would have remained on the streets, committing additional violent crimes.

2. Law Enforcement and Public Benefits

In addition to crime prevention benefits, LPRs may increase officer safety and assist officers in identifying drivers with documented medical conditions who may have driving restrictions, as well as locating missing or abducted persons.

a. Officer Safety

There are three benefits of using LPRs that contribute to officer safety. The first benefit increases fairness and officer safety in policing practices because LPRs assist officers in facilitating non-biased policing. LPRs cannot choose which plates they will scan, and the results are based on information obtained from local, state, and federal databases. Moreover, the technology may reduce racial profiling, which also helps to build trust between police and communities and, thus, creates a safer environment for officers.[112] According to a report by RAND Corporation, LPRs scan every plate and cannot evaluate anything about the occupants of the vehicle.[113]

The second benefit of LPR technology contributes to officer safety as it identifies stolen vehicles or registered owners wanted in connection with past crimes. Such information identified through a vehicle hot-list gives officers a heightened sense of awareness when approaching a vehicle, so officers approach a vehicle with extra caution or request the assistance of additional officers to investigate the vehicle and occupants in question.

---

[111] Baker.

[112] Gierlack et al., *License Plate Readers for Law Enforcement*, 14.

[113] Gierlack et al., 14.

Finally, LPR technology helps officers on patrol concentrate on other tasks, such as driving their patrol cars safely and performing other functions that require an officer to stay alert for potential hazards.[114] In 2017, traffic collisions were the leading cause of deaths, with 47 police officers killed in the line of duty.[115] LPR technology scans vehicle plates, enabling the officer to keep focused on driving.

b. Mental Health Support

Approximately 9.8 million Americans—one out of every 25—experience serious mental-health issues.[116] The significant, sensitive needs of approximately 4 percent of the U.S. population are now better addressed by police departments. In addition to identifying drivers operating vehicles without valid insurance, LPRs can detect registered vehicle owners having suspended or revoked licenses. On March 5, 2018, Dorothy Bruns suffered a seizure while driving in the middle of the day on a Brooklyn street and tragically killed two young children. Officers arrested the vehicle operator and, after a lengthy investigation, charged her with manslaughter, based on information that she had suffered a seizure two months earlier while driving and had been instructed by doctors not to drive for one year.[117] To prevent future tragedies involving drivers operating motor vehicles with known medical conditions that would preclude them from driving, New York City Mayor Bill de Blasio pushed for legislation mandating that doctors notify the Department of Motor Vehicles of drivers with known conditions that could cause them to lose consciousness.[118] LPRs can identify owners operating their vehicles with suspended

---

[114] Moriarty, Criminal Justice Technology, 264–265.

[115] National Law Enforcement Officers Memorial Fund, *2017 End of Year Officer Fatalities Report* (Washington, DC: NLEOMF, 2017), http://www.nleomf.org/assets/pdfs/reports/fatality-reports/2017/2017-End-of-Year-Officer-Fatalities-Report_FINAL.pdf.

[116] "Mental Health by the Numbers," National Alliance on Mental Illness, accessed June 17, 2018, https://www.nami.org/Learn-More/Mental-Health-By-the-Numbers.

[117] Colin Moynihan, "Driver Charged with Manslaughter in Deaths of 2 Children," *New York Times*, May 3, 2018, https://www.nytimes.com/2018/05/03/nyregion/driver-manslaughter-brooklyn-children.html.

[118] "Vision Zero: Mayor de Blasio Pushes for Tougher State Laws to Keep Dangerous Drivers off the Streets," City of New York, March 15, 2018, https://www1.nyc.gov/office-of-the-mayor/news/136-18/vision-zero-mayor-de-blasio-pushes-tougher-state-laws-keep-dangerous-drivers-off-streets#/0.

licenses, and therefore, officers can proactively stop and make a summary arrest, as long as the registered owner is also the operator of the vehicle.

In a 2013 experiment, Lum, Hibdon, Cave, Koper, and Merola evaluated the potential use of LPR technology to identify vehicles being operated by owners with suspended licenses.[119] The evaluation determined that although LPR technology does not act as a deterrent to operate a motor vehicle with a suspended license, it could identify registered owners of vehicles who have suspended licenses and could be stopped and possibly arrested.[120] LPR technology, in conjunction with a collaborative effort with the New York State Department of Motor Vehicles, legislators, and the district attorney's offices, can be leveraged to mitigate similar circumstances in the future. Data that identify individuals with suspended or revoked licenses can be entered into department LPR hot-lists to alert police officers in the field. Officers are legally permitted to stop a vehicle to verify a driver's credentials before taking enforcement action, based on LPR data that identify possible violations or crimes relating to a vehicle or its registered owner.

c. Missing Persons

When law enforcement activates an AMBER alert for a missing child, law enforcement has several methods to alert the public, including digital billboards and cell phones.[121] In addition, if the alert involves a vehicle, law enforcement officers enter the plate number into the LPR hot-list. The New York State Division of Criminal Justice Services has created specific guidelines for dealing with AMBER alerts—specifically how law enforcement should react to ensure the proper dissemination of intelligence.[122] In

---

[119] Cynthia Lum et al., "License Plate Reader (LPR) Police Patrols in Crime Hot Spots: An Experimental Evaluation in Two Adjacent Jurisdictions," *Journal of Experimental Criminology* 7, no. 4 (2011): 321, https://www.voiceofsandiego.org/wp-content/uploads/2018/04/Lum-et-al-2.pdf.

[120] Lum et al., 332.

[121] The AMBER (America's Missing: Broadcast Emergency Response) alert was created in 1996, after nine-year-old Amber Hagerman was kidnapped and tragically murdered.

[122] New York State Division of Criminal Justice Services, *Operation of License Plate Readers in New York State: Suggested Guidelines* (Albany: NYS DCJS, June 2017), 3, https://www.aclu.org/files/FilesPDFs/ALPR/new-york/alprpra_rensselaercountysheriffdepartment_troyny_2.pdf.

addition, the NYPD has established a policy for activating and responding to AMBER alerts, including specific instructions for manual entries, if required.

d. Other Benefits

Local governments also use LPR technology to track commercial carriers, enable payment for tolls on roads, bridges, and tunnels to identify locations with heavy traffic, and estimate travel times to specific highway interchanges.[123] Most toll bridges and tunnels, in addition to E-Z Pass, now use license plate readers to collect tolls, thus eliminating toll plazas. Therefore, without lines of stopped vehicles waiting in cash only-lanes, traffic congestion has eased at area crossings in New York City.

Currently, no laws prohibit private organizations from using LPR technology and creating their own unique databases for their operations. Commercial uses for LPR technology include security and management for school campuses, residences, parking, casinos, airports, and healthcare facilities. Real-time information can identify vehicles that park in unauthorized or restricted areas as well as vehicles that remain on site longer than permitted. Many LPR systems connect to security offices in commercial locations that immediately notify law enforcement if criminal or suspicious activity requires further investigation.

C. CHALLENGES

Law enforcement agencies encounter challenges in using LPR technology. Both citizens and activist groups have raised concerns over privacy, data collection, retention, citizen acceptance, and understanding of the technology, not to mention inaccuracy and misuse. The New York Civil Liberties Union contends that the NYPD's five-year data retention policy for all scanned plates, including plates that are not involved in investigations, is excessive.[124] In addition, the ACLU argues that the NYPD's DAS will track individuals in ways that few citizens can fathom, as the system contains millions of

---

[123] Bryce Clayton Newell, "Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy, and Access to Government Information," *Maine Law Review* 66 (2013): 8.

[124] Hirose, "NYPD's Vast License Plate Reader Database."

data points. Privacy advocates contend that law enforcement agencies can track individuals using LPR scans from moving vehicles, thereby diminishing levels of privacy.[125] Currently, 14 states, not including New York, have laws that regulate the use of LPR technology.[126] The NYPD, however, must continue to address the technology's challenges to retain public support.

1. Privacy

A primary task in law enforcement is balancing the citizens' desire for privacy with the need to keep them safe. Privacy concerns transcend citizen objections over compromised anonymity from police surveillance technologies. Privacy advocates, such as the ACLU, express concern over how law enforcement uses surveillance technologies and how collected data are used, disseminated, and shared with other organizations. Furthermore, LPRs often raise concerns about misuse, in the forms of implicit bias or weak policies and procedures.

a. Data Collection/Invasiveness

The main concerns that the ACLU would like to see addressed include law enforcement's data collection and retention methods. Kaelyn Rich of the New York Civil Liberties Union admits, "LPR can be a reasonably useful technology."[127] Rich also states, "The problem is they're storing records that are not hits. They're keeping these millions of other records on everyday people going about their business. In the United States, it's a core principle that the government does not invade people's privacy and they do not collect information on people in case they do something wrong."[128] New York State has enacted no laws pertaining to LPRs. Bill S23, however, was proposed for LPRs in 2015 and modified in 2017 to include permissible use, collection, and retention of information, as

---

[125] Gierlack et al., *License Plate Readers for Law Enforcement*, 2.

[126] Newell, "Local Law Enforcement Jumps on the Big Data Bandwagon," 402.

[127] Steve Orr, "New York Knows Where Your License Plate Goes," *USA Today*, July 28, 2014, https://www.usatoday.com/story/news/nation-now/2014/07/28/new-york-archiving-license-surveillance-data/13261679/.

[128] Orr.

well as mandatory open-source policies and annual reporting requirements.[129] The bill continues to sit in committee with no definitive path for approval. The only existing New York State document relating to LPRs, the *Suggested Guidelines Manual*, was produced in 2011. Currently, no universal policy exists in New York State. The NYPD, however, has created a detailed policy on LPR use, collection, data retention, and training, which the department has posted on its website.

Merola and Lum have examined the public's perception of LPR technology, surveying a diverse group of citizens to categorize the type of LPR use by the degree of citizen support.[130] The survey revealed that citizens had greater concerns with the dissemination of collected data, retention time, and storage for wide-ranging use but showed little to no concern over the use of LPR technology by law enforcement. Overall, the survey demonstrated support for LPR use—with an existing correlation between individuals who trust law enforcement and those who support LPR technology.

b. Misuse/Abuse of LPR Technology

Critics raise concerns that officers will misuse LPR technology by, for instance, using LPR data for personal use, selectively enforcing laws, and sharing data inappropriately. Critics contend that law enforcement officers may misuse LPR data; the ACLU argues that officers have the ability to patrol with LPR-equipped vehicles and target specific individuals, such as persons engaged in prayer inside a mosque.[131] Such tactics, if conducted at demonstrations, might affect citizens deciding to protest against the government and, thus, negate their right to free speech. Furthermore, critics contend that LPR technology can reveal intimate details for which individuals would plead for anonymity. For example, individuals may be tracked in their vehicles traveling to legal destinations but engaging in secretive activities. Other privacy concerns include the law enforcement use of LPR data to collect information on individuals who may systematically

---

[129] "Senate Bill S23," New York State Senate, last modified December 28, 2016, https://www.nysenate.gov/legislation/bills/2017/S23.

[130] Linda M. Merola and Cynthia Lum, "Understanding Citizen Support for License Plate Readers," *Translational Criminology* (2015): 23, https://www.bja.gov/bwc/pdfs/TC8-Spring2015.pdf#page=25.

[131] Crump, *You Are Being Tracked*, 11.

engage in lawful but private or discreet behavior. In addition, officer misuse of the technology, no matter how infrequent, concerns law enforcement and citizens alike. The ACLU reports several incidents of officers involving criminal misuse of LPR technology.[132]

c. Ineffective Policies

Many law enforcement agencies have written policies that explain LPR rules for officers to follow. Policies vary by agency, with different policies for use, collection, sharing, purging of data, data analysis, and official inquiries into vehicle registrant information. For example, in 2017, 20 states introduced legislation for LPRs; however, no laws were passed.[133] In New York State, several of its counties—Nassau, Suffolk, Westchester, Broome, Albany, Onondaga, Erie, Monroe, and New York City—retain LPR data for five years.

Also, the ACLU contends that the overall return on investment—LPR reads versus LPR hits—is less than 1 percent.[134] The ACLU examined 2009–2011 LPR data from the Minnesota State Patrol and revealed that officers made only 131 arrests and issued 852 citations based on 1.6 million LPR scans.[135] The ACLU contends that most departments maintain LPR data for long periods, and some do not have policies for LPR data whatsoever, even if no open investigations or extenuating circumstances exist.[136] With technology allowing for increased storage capabilities, it is more cost-effective for law enforcement agencies to retain LPR data for longer periods. Further research will dictate whether extended retention periods will pay dividends—if more crimes, such as cold cases, can be solved.

---

[132] Hirose, "NYPD's Vast License Plate Reader Database."

[133] "Automated License Plate Readers: State Legislation 2016 & 2017," National Conference of State Legislatures, accessed May 6, 2018, http://www.ncsl.org/research/telecommunications-and-information-technology/automated-license-plate-readers-state-legislation-2016.aspx.

[134] Crump, *You Are Being Tracked*, 15.

[135] Crump, 15.

[136] Crump, 16.

d. Data Storage, Data Sharing, and Hacking

The security of sensitive data challenges government agencies, law enforcement, and the private sector. LPR information is considered big data, which are defined as "data sets that are so large or complex that primitive data processing application software is inadequate to deal with them."[137] The sheer number of vehicles being scanned on roadways throughout the United States means LPRs require an abundance of storage space. In addition, sharing of data across government and law enforcement agencies increases the potential for cyber-attacks. Recent history demonstrates that cyber-attacks result in serious damage to company credibility and individual privacy of sensitive, personal information. Big data breaches—Yahoo in 2013 affecting 1.5 billion user accounts, eBay in 2014 affecting 145 million users, and J.P. Morgan Chase in 2014 affecting 76 million households and seven million small business—all create trust issues and create massive financial burdens for both corporations and individuals.[138] Compromised LPR data can reveal vehicle locations, such as for individuals who frequent locations they wish to keep private, as well as historical data, such as red light and speed camera violations. For example, in 2015, over 100 LPR cameras from various law enforcement agencies in different states were left unsecured online, and anyone with an internet connection and a browser had unlimited access to their data.[139]

2. Accuracy

LPR technology faces problems with overall reliability. Examples include dirty license plates, intentional alteration of plates, and identical vanity plates issued in different states.[140] Reliability, accuracy, and overall performance concerns are not unique to the use

---

[137] Surbhi Jain, "Big Data: What, Why and Why Not," *International Journal of Engineering Development* 5, no. 2 (2017): 5, https://www.ijedr.org/papers/IJEDR1702334.pdf.

[138] Jain, 5.

[139] Cooper Quintin and Dave Maass, "License Plate Readers Exposed! How Public Safety Agencies Responded to Major Vulnerabilities in Vehicle Surveillance Tech," Electronic Frontier Foundation, October 28, 2015, https://www.eff.org/deeplinks/2015/10/license-plate-readers-exposed-how-public-safety-agencies-responded-massive.

[140] Gierlack et al., *License Plate Readers for Law Enforcement*, 15.

of LPR technology. Other law enforcement technologies, such as BWCs, experience similar concerns and are continuously addressed.

LPRs sometimes fail to read damaged or obscured license plates or those covered with transparent materials, such as clear license plate covers.[141] Mobile LPR readers can mistakenly extract street addresses and street signs and erroneously record them as license plates, thereby populating databases with inaccurate data.[142] In the case of extracting LPR data from large crime scenes, crime analysts spend needless hours sifting through and disaggregating legitimate information from erroneous data.

a. False Positives, False Negatives, and Misreads

When LPRs scan plates that result in false positives, the overall accuracy of the collected data can be affected. Although most LPRs are accurate, misreads do occur, and readers may have difficulty in differentiating between identical license plates from different states.[143] This may have serious ramifications for both citizens and law enforcement. For example, if a complainant reports a stolen vehicle with a plate identical to one issued by another state, it may create a false positive and identify the wrong vehicle as being stolen. To address this concern in the NYPD, officers are tasked with verifying all information before taking enforcement action.

b. Intentional Circumvention

Private companies are investing heavily in solutions to circumvent LPR technology intentionally. Laws that were passed decades ago to prevent intentional circumvention, such as license plate covers and jammers that scramble the signal emitting from the LPR, have failed to keep up with new technologies. Some companies claim their devices will prevent an LPR from scanning the plate.[144] Phantom Plate has designed a spray-on, high-

---

[141] Gierlack et al., 15.

[142] Gierlack et al., 15.

[143] Gierlack et al., 15.

[144] "SunflexZone Anti-ALPR & Red-Light Camera Privacy Solutions," Sunflex Zone, accessed June 9, 2018, https://www.sunflexzone.com/.

powered gloss that over-exposes the images of the license plate and, therefore, intentionally circumvents the LPR.[145] Other companies sell products, such as clear sprays, that can be applied over a plate to avoid an LPR.[146] This technology can thwart law enforcement efforts to enforce speeding, control intersections, and identify stolen vehicles.

3. Transparency and Public Trust

The ACLU recently filed legal action against the U.S. Immigration and Customs Enforcement (ICE) for failure to provide records on how the agency uses LPR data.[147] The ACLU expressed concern about how ICE stores and uses the data for civil immigration enforcement. These concerns have damaging effects on citizen support of law enforcement. Although ICE has announced the purchase of LPR data on its website and assured citizens that "the agency complies with privacy and civil liberties requirements," the organization explains LPR data are leveraged to "support criminal and administrative law enforcement missions."[148] LPR use by ICE is a smaller concern of a larger immigration issue. In January 2018, 18 citizens, including two New York City council members, were arrested by the NYPD following a demonstration over the immigration status of an individual.[149] The incident highlights the public's greater focus on how law enforcement collects all data, including LPR scans, and whether it uses the data against citizens.

---

[145] "Avoid Red Light and Speed Camera Tickets," Phantom Plate, accessed April 20, 2018, https://www.phantomplate.com/.

[146] "Avoid Red Light and Speed Camera Tickets," Photo Blocker, accessed April 21, 2018, https://www.photoblocker.com/photoblocker.html.

[147] Sophie Haigney, "ACLU Sues Immigration and Customs Enforcement for License Plate Reader Records," SF Gate, May 28, 2018, https://www.sfgate.com/bayarea/article/ACLU-sues-ICE-for-license-plate-reader-contracts-12937712.php.

[148] U.S. Immigration and Customs Enforcement, *Acquisition and Use of License Plate Reader Data from a Commercial Service*, DHS-ICE-PIA-039 (Washington, DC: Department of Homeland Security, December 2017), https://www.dhs.gov/publication/dhs-ice-pia-039-acquisition-and-use-license-plate-reader-data-commercial-service.

[149] Liz Robbins, "Activists and ICE Face Off over Detained Immigrant Leader," *New York Times*, January 12, 2018, https://www.nytimes.com/2018/01/12/nyregion/immigration-activist-deportation.html.

a. Transparency by Law Enforcement

Critics have requested that the NYPD become more transparent with its policing strategies and policies. In an effort to mitigate those concerns, the NYPD uses social media applications such as Facebook, Instagram, Twitter, and the department's webpage to promote transparency. In addition, the department publishes reports, statistics, and policies online for public consumption. In March 2018, the NYPD updated its LPR policy and published it online to reflect the latest advancements of the technology. The policy explains,

> The LPR system allows for the proactive entry of license plate numbers and partial plate numbers, enabling the system to activate when the wanted vehicle's license plate has been read by the LPR device. The Real Time Crime Center can be contacted to conduct a search of past records of license plate numbers searched. LPR devices are intended to provide access to stolen and wanted files and may also be used in furtherance of a criminal investigation. The use of an LPR device for any other purpose is strictly prohibited.[150]

The new policy informs officers and citizens of its zero-tolerance policy for officer misuse of LPR technology. While the NYPD has specific guidelines for citizens to obtain BWC videos to meet citizen expectations of transparency, there are no specific instructions for citizens to obtain LPR data concerning their vehicles.

In 2014, the NYPD denied a Freedom of Information Law inquiry from the New York Civil Liberties Union, which requested detailed information on LPR use, collection, sharing, locations and number of units, as well as the number of scans, officer training, and EZ-pass data among other concerns.[151] The NYPD denied the request, explaining that the release of LPR data would interfere with law enforcement investigations and disclose sensitive techniques and procedures that might endanger the safety of citizens.[152] In addition, the denial cited Public Officers Law (POL) §87(2)(e)–(g) and (i), which exempt

---

[150] NYPD, *Patrol Guide: "Padlock Law."*

[151] City of New York, Police Department Legal Bureau, "Freedom of Information Law Request: #14-PL-0175" (letter to Nate Vogel, New York Civil Liberties Union, April 17, 2014), https://www.nyclu.org/sites/default/files/20140417_NYPDDenial_NYCLUFOILRequest.pdf.

[152] City of New York, Police Department Legal Bureau.

such records from release.[153] Prioritizing safety and remaining transparent is challenging for law enforcement, especially when the public interprets surveillance technologies as deceptive tactics.

b. Community Mistrust and Acceptance

There seems to be a greater degree of acceptance for LPRs than other law enforcement surveillance technologies. The NYPD created and updated strong policies and procedures governing the use of LPR technology, which mitigated most concerns of mistrust among the community. Growing public acceptance and increased transparency have contributed to the capabilities of LPR technology because citizens today are better informed and more apt to challenge traditional methods of policing. Citizens have been aware of the benefits of LPR technology, such as its use in expediting traffic flow and easing congestion on area bridges and tunnels, ever since toll collection booths were replaced with fixed LPRs. Nevertheless, LPR systems work in conjunction with other technologies that are not governed by police departments, creating the potential for new privacy concerns.

In June 2018, California began piloting license plates that digitally display the plate number as well as commercial advertisements; the digital plates also transmit location data for future analysis and record driving habits.[154] The benefits are that the plate pays tolls automatically, tracks stolen vehicles, tracks mileage, and receives virtual boundary notifications. This new technology also receives notification from such public service messaging as street closures and AMBER alerts. These benefits, however, may erode personal privacy. Stephanie Lacambra from the Electronic Frontier Foundation contends that vehicle location data have "the potential to reveal a lot more than . . . where you happen to be at a particular moment in time."[155] Although the capabilities of the digital license

---

[153] City of New York, Police Department Legal Bureau.

[154] James Doubek, "Digital License Plates Roll Out in California," NPR, June 1, 2018, https://www.npr.org/sections/thetwo-way/2018/06/01/616043976/digital-license-plates-roll-out-in-california.

[155] Doubek.

plate may sacrifice citizen privacy by sharing all of the metadata associated with a vehicle, the pilot is voluntary and offers benefits for both citizens and law enforcement.

D. CONCLUSION

LPR technology continues to evolve, thereby creating additional uses for law enforcement and the private sector. Initially, LPR technology enabled law enforcement to track stolen vehicles. New uses of LPR technology include toll collection, summons enforcement, and monitoring of traffic conditions. LPR technology assists law enforcement in reducing and investigating crimes and terror attacks, increasing officer safety, locating missing persons, and supporting individuals with sensitive needs. In addition, private companies are using LPR technology to inventory vehicles parked in lots and garages, as well as scanning plates to identify scofflaws on the road or vehicles subject to repossession.[156] Roberts and Casanova contend that LPR technology has a positive impact on the law enforcement community and deems it successful in multiple uses.[157]

While no technology exists without some shortcomings, LPR has proven beneficial to law enforcement despite some systematic flaws. An amalgamation of FRT and LPR technologies may appear in the near future, as suggested with the high-occupancy vehicle example. In the near the future, FRT will likely be used to identify faces in high-occupancy vehicle lanes on area highways to determine whether the appropriate number of people are inside the vehicle.[158] It is unknown, however, how law enforcement will construct additional methods to leverage both LPR technology and real-time FRT for the benefit of the public and law enforcement.

In exchange for improved traffic conditions, though, citizens may begin to feel diminished levels of privacy—yet such LPR applications as summons enforcement and

---

[156] Kaveh Waddell, "How License-Plate Readers Have Helped Police and Lenders Target the Poor," *Atlantic*, April 22, 2016, https://www.theatlantic.com/technology/archive/2016/04/how-license-plate-readers-have-helped-police-and-lenders-target-the-poor/479436/.

[157] Roberts and Casanova, *Automated License Plate Recognition*.

[158] Dave Maass, "The Four Flavors of Automated License Plate Reader Technology," Electronic Frontier Foundation, April 6, 2017, https://www.eff.org/deeplinks/2017/04/four-flavors-automated-license-plate-reader-technology.

crime fighting mutually benefit law enforcement and citizens. Furthermore, citizens are living in a society connected by technology, social media, and the internet. The paradigm that defines their acceptance of new privacy levels has yet to be determined.

THIS PAGE INTENTIONALLY LEFT BLANK

III. FACIAL RECOGNITION TECHNOLOGY

Like LPR technology, FRT—especially when used in real time—has the advantage of acting as a force multiplier for the NYPD in crowded environments such as the New York City subway system. LPRs and FRT are similar technologies, so they share many of the same advantages and disadvantages. The NYPD mitigated many of the challenges of LPRs and could ostensibly apply the same framework to address the challenges of real-time FRT. This chapter provides an overview of FRT, including the history and definition of the technology, reviews FRT applications, and describes how the benefits will outweigh the risks. Finally, it addresses the concerns over how law enforcement will collect, share, and disseminate personal information obtained from facial recognition software.

A. OVERVIEW

In the 1960s, Woodrow W. Bledsoe developed the first semi-automatic face recognition system.[159] This method identified the ears, eyes, nose, and mouth on photographs and then calculated the distances and ratios to compare features to source reference data.[160] FRT processes and matches the unique characteristics for identification or authorization. FRT uses a digital or video camera that enables the software to detect images of unknown individuals, analyze the features within the images, and compare those analyzed features to images of known individuals within a database.[161] FRT is similar to other *biometrics*, such as fingerprints, iris scans, and voice recognition.

Fifty years after its invention, FRT has integrated into our everyday lives, creating new societal benefits around the world. With recent advancements in FRT, law enforcement, the federal government, and the private sector all look to leverage the technology to make their operations more secure, more efficient, and—in some cases—

---

[159] Woodrow Wilson Bledsoe, *Proposal for a Study to Determine the Feasibility of a Simplified Facial Recognition Machine* (Palo Alto, CA: Panoramic Research, January 30, 1963), http://archive.org/details/
firstfacialrecognitionresearch.

[160] Bledsoe.

[161] Find Biometrics, "Facial Recognition."

more profitable. The greatest change in FRT in the last decade is its ability to accurately identify persons in real time. While real-time technology has the potential to change modern policing with significant public benefits, leadership must proactively address the resulting challenges.

B. BENEFITS OF FRT

Facial recognition is a non-intrusive biometric technology, meaning that facial recognition systems can scan faces without citizen participation and, when used in real time, identify people as they walk. Citizens do not need to stop walking or look directly into a camera, so real-time FRT can act as a force multiplier for the NYPD in the New York City subway system by monitoring the ridership in all 472 stations. If real-time FRT existed in the subway, the NYPD could instantly screen millions of passengers each day—identifying both wanted criminals and suspected terrorists—but without unnecessary personal intrusions, such as bag checks and container screenings, during peak operational hours. Public safety benefits accentuate the greater good that real-time FRT can provide law enforcement. Figure 2 depicts how FRT algorithms match images against a database.

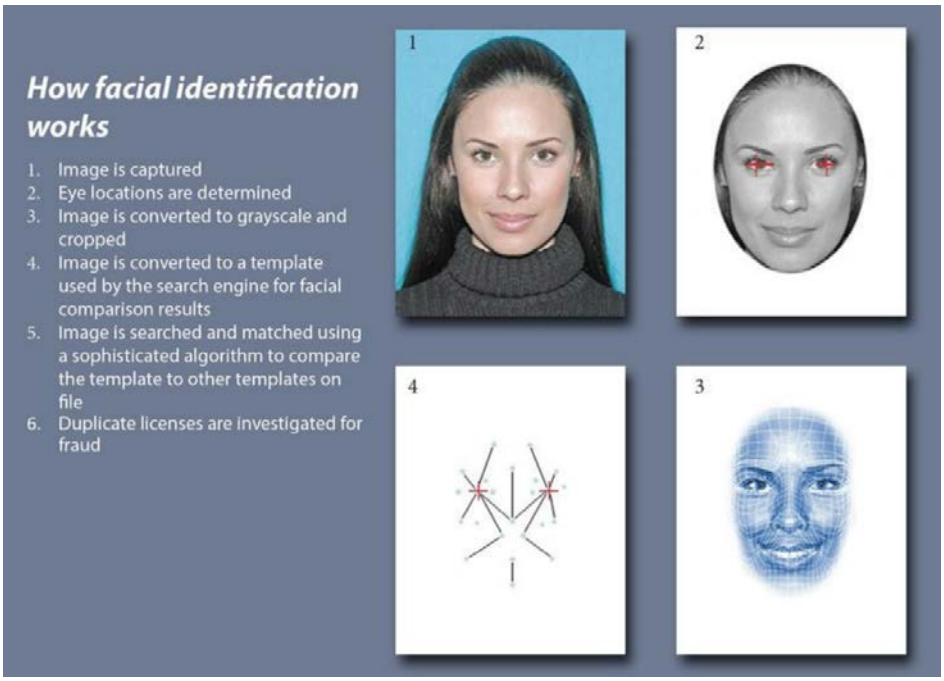

Figure 2. Algorithm for Matching Facial Images[162]

In law enforcement, leadership needs to evaluate technology when opportunities arise to make officers more efficient, better informed, and safer. Allevate, a company that promotes enhanced safety and operational efficiency, contends that recent acts of terrorism around the world demonstrate less sophistication but increased frequency.[163] The company argues that technology can play a critical role in improving the efficiency of law enforcement and intelligence agencies and furthering the ability to interrupt future terror plots.[164] Technology has changed the way people think of traditional business models. Throughout history, law enforcement has often been astute in using technology to combat crime. For example, law enforcement has leveraged technologies, such as the automobile, the telephone, and more recently, biometric technology to create significant efficiencies. According to one law enforcement scholar, technology in policing "helped emphasize

[162] Source: Jennifer Lynch, *Face Off, Law Enforcement Use of Face Recognition Technology* (San Francisco: Electronic Frontier Foundation, February 12, 2018), 5, https://www.eff.org/wp/law-enforcement-use-face-recognition.

[163] "Helping to Counter the Terrorist Threat Using Face Recognition," Allevate, July 28, 2017, http://allevate.com/index.php/2017/07/28/helping_to_counter_the_terrorist_threat_using_face_recognition/.

[164] Allevate.

discipline, equal enforcement of the law and centralized decision making."[165] Until 10 years ago, it would have been crazy to think of starting a hotel business without hotels, a taxi company without cabs, or a merchandise company without stores in which to shop, but today such innovators as Airbnb, Uber, and Amazon have changed the way companies think and function.[166] These same principles apply to law enforcement, which requires abstract thinking to solve problems, create additional efficiencies, and foster stronger community relationships. Figure 3 indicates the process by which FRT generally operates.

---

[165] Seaskate, *The Evolution and Development of Police Technology* (Washington, DC: Seaskate, July 1, 1998), https://www.ncjrs.gov/pdffiles1/Digitization/173179NCJRS.pdf.

[166] William D. Eggers, *Delivering on Digital: The Innovators and Technologies That Are Transforming Government*, 1st ed. (New York: Rosetta Books, 2016), loc. 79–121.

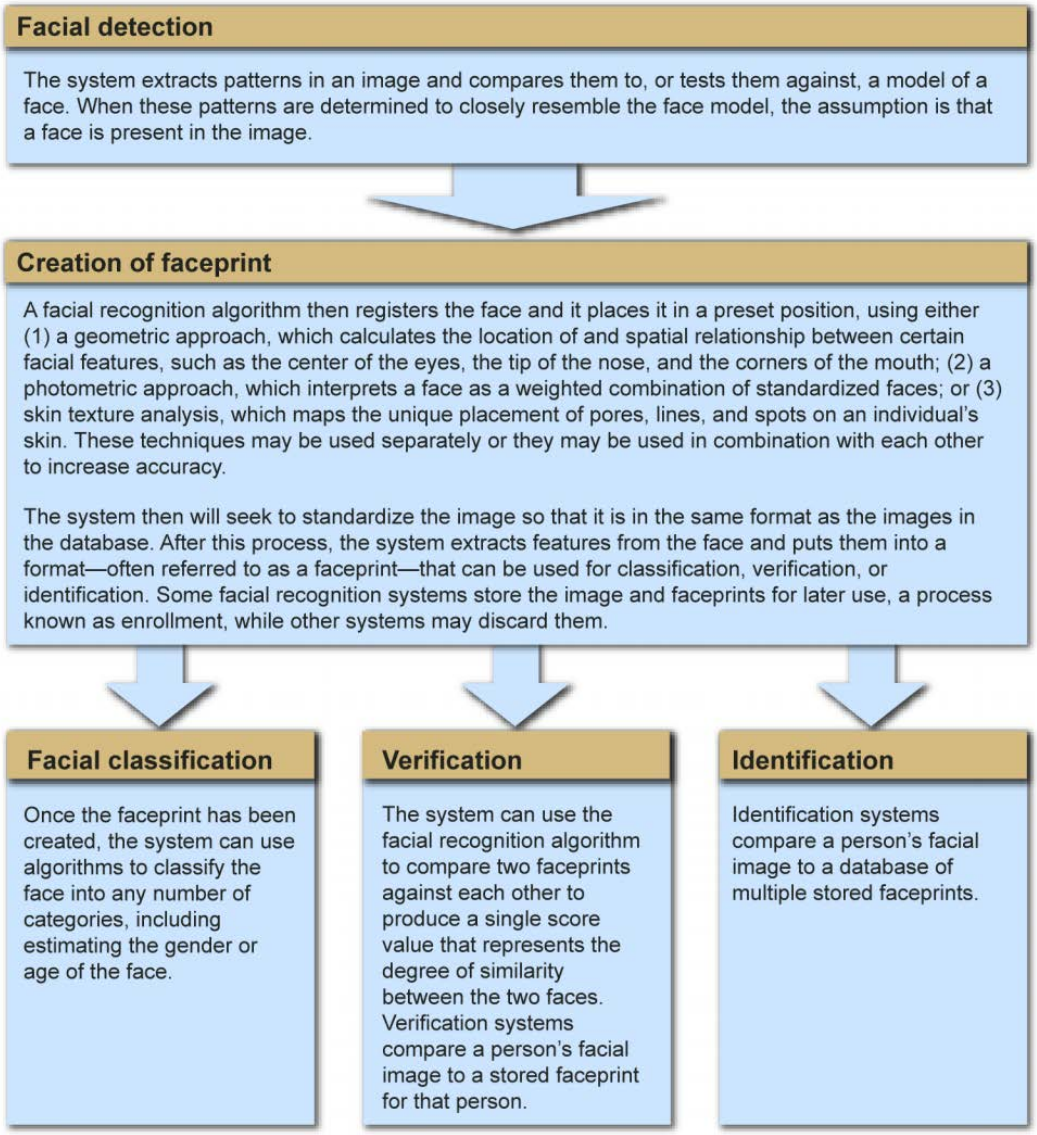

Figure 3. How FRT Systems Generally Work[167]

1. Crime Prevention Benefits

The most important benefits derived from the use of FRT all involve preventing or reducing crime. Although the use of FRT already benefits the NYPD, if the department

[167] Source: Government Accountability Office, *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law*, GAO-15-621 (Washington, DC: GAO, July 2015).

uses FRT in real time, crime reduction benefits—potentially terrorism prevention and rapid wanted person identifications—grow exponentially.

a. Preventing Violent Crime

Law enforcement began piloting real-time FRT for large events and, over time, expanded its use at demonstrations and transportation systems. The first use of real-time FRT in the United States occurred during the Super Bowl in 2001; law enforcement screened 100,000 people using FRT—among whom 19 people were arrested due to active arrest warrants.[168] This pilot was the first of its kind at a high-profile event. More recently, police are beginning to revisit the idea of using real-time FRT at large, high-profile events. In 2017, the Metropolitan Police in London deployed real-time FRT to scan crowds at a remembrance ceremony. The database contained 50 individuals known for exhibiting compulsive behavior toward public figures. Although none of the individuals was wanted for prior crimes, it was a proactive approach to mitigating potential safety concerns at large-scale, high-profile events.[169]

In more modern times, real-time FRT has the capability to stop criminals who commit serial violent crimes. On May 13, 2015, David Baril attacked NYPD Police Officer Lauren O'Rourke with a hammer in midtown Manhattan when O'Rourke and her partner approached Baril to arrest him. He was wanted for a string of serious robberies in Manhattan, striking his victims in the head with a hammer and attempting to remove property.[170] Baril had already been a wanted criminal with an active arrest warrant prior to his recent pattern of robberies. Following his latest robbery, NYPD detectives combed the area for clues. After examining CCTV videos of the Herald Square Subway Station's platforms and turnstiles, detectives observed an individual on video inside of the subway

---

[168] Daniele Cavadini et al., "Introducing the Biometrical Electronic Passport (EPass)" (seminar, University of Fribourg, 2008), 8.

[169] Mark Townsend, "Police to Use Facial-Recognition Cameras at Cenotaph Service," *Guardian*, November 11, 2017, http://www.theguardian.com/technology/2017/nov/12/metropolitan-police-to-use-facial-recognition-technology-remembrance-sunday-cenotaph.

[170] J. David Goodman and Al Baker, "Police Shoot Hammer-Wielding Man Sought in 4 Manhattan Attacks," *New York Times*, May 13, 2015, https://www.nytimes.com/2015/05/14/nyregion/officer-shoots-man-in-midtown-manhattan.html.

station that matched a description provided by the victim. The robbery victim was able to identify the photo as the individual who attacked him.

The NYPD's Facial Identification Section identified Baril using FRT and disseminated his picture onto the department smartphones issued to every police officer. Two days later, Baril was walking in midtown Manhattan when Officer O'Rourke observed him. While FRT was attributed with Baril's initial identification, real-time FRT could have identified Baril earlier as a wanted criminal, which would have resulted in his immediate apprehension and thereby protected citizens from additional acts of violence. One of the primary benefits of real-time FRT in contrast with FRT, as a post-investigative crime-fighting strategy, is the ability for law enforcement to identify wanted career felons and apprehend them in crowded environments before they commit additional violent crimes.

b. Investigating and Preventing Acts of Terrorism

Real-time FRT can also identify and alert police officers to the presence of a known terrorist entering or exiting a specific location. In the New York City subway system, a real-time system would enable NYPD police officers to screen millions of people each day and potentially identify individuals on terror watch lists. Other parts of the world are evaluating real-time FRT systems. In Germany, police in Berlin are testing real-time FRT in the Berlin Train Station, contending that the technology can alert police of known terrorism suspects.[171]

Although no acts of terrorism have been successfully prevented using real-time FRT, law enforcement professionals sense that because of recent technological advancements, using real-time FRT may prevent an act of terrorism. For example, following the London terror attacks at the Borough Market on June 28, 2017, former MI5 Chief Johnathan Evans claimed, "The attacks . . . were very likely preceded by reconnaissance activity, and one can envisage that the use of FRT would be able to identify

[171] Justin Huggler, "Facial Recognition Software to Catch Terrorists Being Tested at Berlin Station," *Telegraph*, August 2, 2017, http://www.telegraph.co.uk/news/2017/08/02/facial-recognition-software-catch-terrorists-tested-berlin-station/.

that in advance and enable preemptive action to be taken."[172] Although several law enforcement agencies around the world are currently testing real-time FRT, further research is necessary before both law enforcement and facial recognition software companies can assert conclusive findings of its effectiveness.

c. Real-Time Identifications of Wanted Persons and Known Suspects

FRT is increasingly being used as a real-time application to identify wanted persons and known suspects. Instant identifications of individuals have the potential benefits of making the airline industry safer, locating missing children and adults, and helping instantly to apprehend individuals wanted for serious crimes. Several companies contend that real-time FRT is advanced enough for use on a variety of platforms, for the military, law enforcement, and the private sector. Technology companies NEC (NeoFace Watch) and Cognitec both specialize in real-time FRT and contend that their facial recognition software is accurate with real-time functionality, regardless of various angles and lighting.[173] According to NEC, NeoFace Watch mitigates challenges such as "crowded environments, poor lighting, moving subjects and multiple variables as small yet significant as spectacles, hats, and scarves."[174]

An additional benefit of the real-time use of FRT is the ability to identify wanted and missing persons. In November 2016, Safran Identity & Security, formerly Morpho, collaborated with INTERPOL to create a database of facial images. Both parties recognized the opportunities that this ever-expanding biometric science brought to law enforcement. Now there is a tool available to law enforcement that can be used globally to identify missing and wanted persons, as well as persons of interest. INTERPOL intends to take the

---

[172] "Facial Recognition Technology 'Could Prevent Future Terror Attacks,'" ITV News, March 1, 2018, http://www.itv.com/news/london/2018-03-01/facial-recognition-technology-could-prevent-future-terror-attacks/.

[173] Rawlson O'Neil King, *Special Report: Biometrics in Law Enforcement* (Lansing, MI: Biometrics Research Group, Michigan State University, 2017), 1–3, https://www.biometricupdate.com/wp-content/uploads/2017/08/special-report-biometrics-in-law-enforcement.pdf.

[174] NEC Global Face Recognition Centre of Excellence, *NeoFace Watch, High Performance Face Recognition* (NEC Global Face Recognition Centre of Excellence, 2016), https://www.nec.com/en/global/solutions/safety/face_recognition/PDF/Face_Recognition_NeoFace_Watch_Brochure.pdf.

project to the next phase by enhancing in-field operations, allowing certain photos to be accessible on smart devices. Once it enacts this change, INTERPOL can use that data to check faces against specific watch lists in real time.[175]

In addition, major transportation facilities in the United States are beginning to test FRT. On October 11, 2017, U.S. Customs and Border Protection began a pilot program using FRT to screen passengers arriving and departing John F. Kennedy Airport in New York City.[176] John Wagner, deputy executive assistant commissioner of the Office of Field Operations, explains, "As we continue to deploy technical demonstrations, CBP is assessing the use of biometric technology as part of a future end-to-end process, from check-in to departure, in which travels use biometrics instead of their boarding pass or ID throughout the security and boarding process."[177]

d. Investigative Assistance

The NYPD has the capability to leverage FRT for use in real time, but currently, the NYPD is not using any form of real-time FRT. The department does use FRT, however, as a post-investigative tool to identify perpetrators involved in crimes and to identify deceased and unidentified persons. The NYPD's Facial Identification Section (FIS) has existed since 2011 and operated as a subunit under the Real Time Crime Center. It operates as an investigative mechanism for detectives in the field, and their mission is to provide investigative leads to assist detectives in identifying unknown individuals related to investigations through biometric algorithms, intelligence data, social media, and any other investigative means. Individuals with moderate disfigurements can still be analyzed and identified by detectives using FRT software. Precinct commanders and detective squad commanders utilize the resources of FIS to aid in criminal investigations in which the perpetrator is unidentified. In addition, FIS detectives leverage social media to help identify

---

[175] "Forensics," INTERPOL, accessed July 3, 2018, https://www.interpol.int/INTERPOL-expertise/Forensics/Facial-recognition.

[176] "CBP Deploys Facial Recognition Biometric Technology at 1 TSA Checkpoint at JFK Airport," Customs and Border Protection, October 11, 2017, https://www.cbp.gov/newsroom/national-media-release/cbp-deploys-facial-recognition-biometric-technology-1-tsa-checkpoint.

[177] Customs and Border Protection.

unknown perpetrators. Facebook and Instagram have a database of pictures larger than that of all Department of Motor Vehicles (DMV) and FBI databases combined.[178]

FIS works with the private sector and other city agencies to educate them on camera placement, video quality, and methods used to read faces, so FRT software can successfully process and analyze the image. FIS, however, is still subject to scrutiny. In 2018, Georgetown University's Center on Privacy and Technology filed a lawsuit against the NYPD, stating the department's "face-recognition system appears to include data for every NYPD arrestee, meaning that each arrestee is subjected to face-recognition searches."[179] In addition to the NYPD database, the New York State DMV maintains a massive photo database. Although several states use their respective DMV databases to conduct searches, the NYPD does not currently use DMV photographs for database comparisons. The New York State DMV, however, as well as the Department of Motor Vehicles in 39 other states use FRT to categorize over 16 million photos to assist in detecting fraudulent licenses.[180] In New York State, the program began in January 2017, and Governor Cuomo says it "has led to the arrest of 100 suspected identity thieves and opened an additional 900 unsolved cases."[181] There is strong evidence to show that as FRT evolves, criminals are easier to detect and the evidence required in establishing probable cause is easier to obtain.

---

[178] Tom Risen, "Could the FBI See Your Selfies?," *U.S. News & World Report*, July 8, 2014, https://www.usnews.com/news/articles/2014/07/08/fbi-may-seek-facebook-data-for-facial-recognition.

[179] Steven Rex Brown, "NYPD Ripped for Abusing Facial-Recognition Tool," *New York Daily News*, March 1, 2018, http://www.nydailynews.com/new-york/nyc-crime/nypd-ripped-abusing-facial-recognition-tool-article-1.3847796.

[180] David Kravets, "Enhanced DMV Facial Recognition Technology Helps NY Nab 100 ID Thieves," *Ars Technica*, August 28, 2016, https://arstechnica.com/tech-policy/2016/08/enhanced-dmv-facial-recognition-technology-helps-ny-nab-100-id-thieves/.

[181] "Governor Cuomo Announces More Than 100 Arrests since Major Enhancement to DMV's Facial Recognition Technology," New York State Governor's Office, August 24, 2016, https://www.governor.ny.gov/news/governor-cuomo-announces-more-100-arrests-major-enhancement-dmvs-facial-recognition-technology.

2. Law Enforcement and Public Benefits

In addition to crime-prevention benefits, real-time FRT may increase officer safety, assist officers in the field when interacting with individuals who cannot care for themselves, and help locate missing persons.

a. Officer Safety

Although no specific research correlates FRT to officer safety, the possibility exists that if FRT can integrate with other technologies, such as LPR and BWC technologies, officers will have more information when interacting with individuals, such as persons wanted for murder or who have prior arrests for assaulting police officers. In addition, officer stops can be expedited if citizen identifications are validated in the field. For example, Transit NYPD officers sometimes wait 30–45 minutes for a marked patrol vehicle to transport an individual back to the station house solely to ensure proper identification prior to issuing a summons. If FRT could properly identify a person in the field, a police officer can issue a summons on the scene, thereby saving valuable time for both citizens and police officers. In addition, officers face increased risks when waiting for a vehicle to transport the perpetrator. Increased wait times may lead to avoidable confrontations, officers being assaulted, or perpetrators attempting to escape custody.

b. Mental Health Support

In addition to crime-fighting benefits, FRT—especially when used in real time—can assist officers in helping individuals who might be unable to care for themselves. FRT can immediately alert officers of potential special needs of the individual with whom they are interacting. In California, the San Diego County Sheriff's Department uses FRT to assist citizens with disabilities such as autism, dementia, Alzheimer's, down syndrome, or any other condition.[182] The Take Me Home Program provides officers with emergency contact information, physical conditions, and special needs to help the individual.[183] FRT

---

[182] "Home Page," San Diego County Sheriff's Department, accessed May 29, 2018, 1–2, http://www.sdsheriff.net/tmh/docs/tmh-english.pdf.

[183] San Diego County Sheriff's Department, 2.

provides officers with potentially life-saving information in the event that the individual is unable to communicate. For example, if officers encounter an unconscious person, FRT could search the database for a match and ascertain critical information, including but not limited to allergies, use of a pacemaker, or contact information for a relative.

c. Missing Persons

Law enforcement could benefit from the use of real-time FRT if missing persons were included in the database. In 2017, there were 651,226 persons reported missing in the United States.[184] In 2009, for example, 13-year-old Francisco Hernandez Jr. was reported missing in New York City. Hernandez, diagnosed with Asperger syndrome, spent 11 days in the New York City subway system before he was finally located by a police officer.[185] Hernandez was underground most of the time, wandering around subway stations and riding different trains. He was ultimately identified by a transit police officer, who recognized the boy from missing person posters in the subway. There is a strong possibility that, if real-time FRT had existed in the New York City subway system, Hernandez could have been located sooner. If the NYPD had used real-time FRT, the NYPD detectives could have entered the boy's photograph into the facial recognition database from the moment the boy's mother reported her son missing. If Hernandez had walked by any of the thousands of cameras located in the subway system, real-time FRT would have alerted police to his exact location.

In 2017, a six-year-old girl was reported missing in China, and the only documentation provided to police was an old photo, taken several years earlier. Police were able to locate the missing girl quickly through an advanced web of cameras linked with real-time FRT.[186] The system, produced by Skynet, is 99.8 percent accurate and can scan

---

[184] "2017 NCIC Missing Person and Unidentified Person Statistics," Federal Bureau of Investigation, accessed June 17, 2018, https://www.fbi.gov/file-repository/2017-ncic-missing-person-and-unidentified-person-statistics.pdf/view.

[185] Jamie Guzzardo and Jesse Solomon, "Missing Boy Spent 11 Days Wandering New York Subways," CNN, November 25, 2009, http://www.cnn.com/2009/US/11/25/new.york.subway.teen/index.html.

[186] "'Skynet' System Supported by Facial Recognition Technology Boosts Chinese Public Safety" People's Daily Online, March 26, 2018, http://en.people.cn/n3/2018/0326/c90000-9441798.html.

faces regardless of angles and lighting. In addition, Skynet claims exceptional system performance in apprehending perpetrators who commit violent crimes such as homicides, robberies, or abductions.[187]

d. Overcrowding in Transit

One of the many challenges for subway riders entering the New York City subway system is its antiquated payment systems and burdensome points of entry. Citizens often experience long lines, especially during morning and afternoon rush hour and when purchasing a daily, weekly, or monthly fare, known as a MetroCard. Individuals can purchase MetroCards from vending machines or from booth clerks, located near subway entrances. The current system creates long lines for frustrated customers waiting to purchase a MetroCard, who are then forced to wait while each person swipes for access to the subway. In addition, long lines can create opportunities for criminals. Pickpocketing and other similar crimes occur when customers juggle multiple items, such as wallets, cell phones, credit cards, or cash, in order to purchase a MetroCard from a vending machine.

Just as technology has advanced from the subway token to the MetroCard, the next revolutionary payment method could become real-time FRT. A company in the United States began testing real-time FRT for instant payment and access into subway systems. Such a system would eliminate the need for MetroCard vending machines and cumbersome turnstiles and gates.[188] Long lines caused by individuals with expired or damaged MetroCards, or those unfamiliar with their use, would be replaced with an open walkthrough area that processes payments as persons walk into the subway system. This technology is similar to recent changes made at New York City tunnels and bridges. Toll plazas were eliminated at all bridges and tunnels, reducing traffic congestion. Vehicle payments are processed through E-Z Pass or LPRs, which photograph the license plate. Figure 4 illustrates the notional use of FRT in mass transit settings.

---

[187] People's Daily Online.

[188] Tammy Waitt, "CUBIC Testing Face Recognition for Subway (Learn More, Video)," American Security Today, October 10, 2017, https://americansecuritytoday.com/cubic-testing-face-recognition-subway-learn-video/.

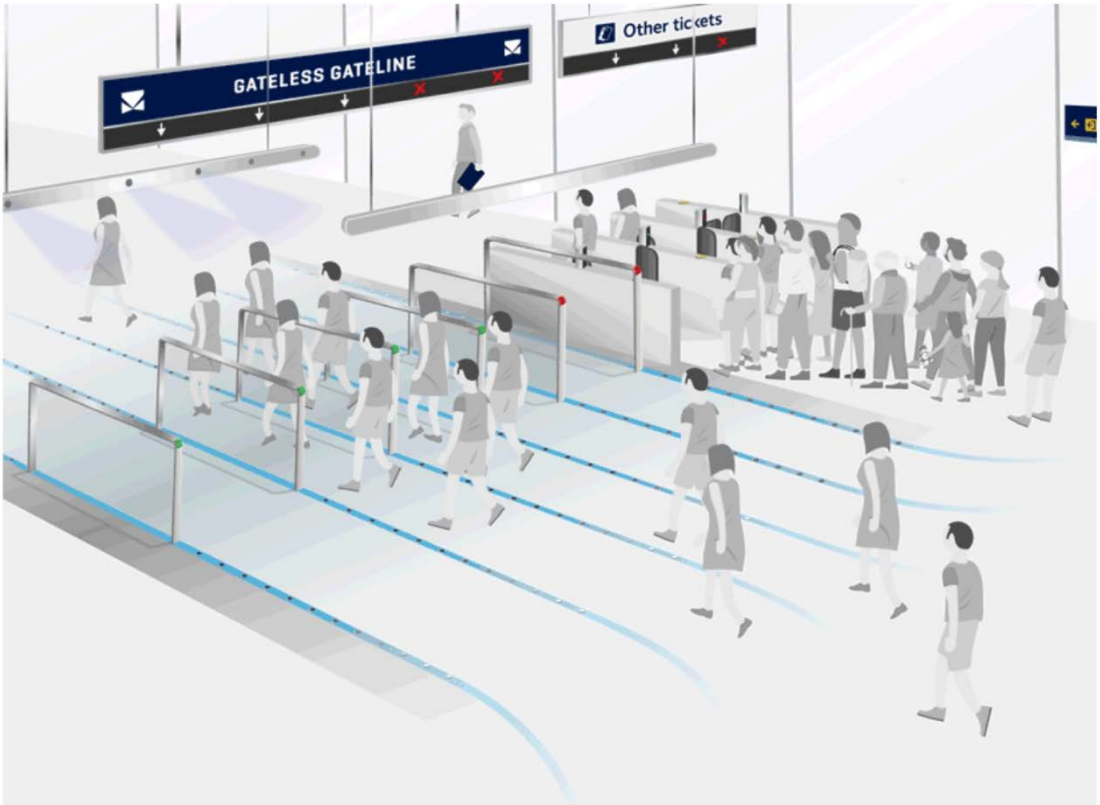

Figure 4. The Gateless Gate Line Concept Using FRT[189]

e. Integration with Other Technologies

FRT could also be integrated with other existing law enforcement technologies such as LPRs, BWCs, drones, and smartphones. For example, New York State legislators are evaluating the potential for LPRs to work in tandem with FRT in New York State tunnels and bridges.[190] A vast and interconnected camera system would identify vehicles and persons entering and exiting New York City. Lynn Gore, deputy chief procurement officer for the Metropolitan Transit Authority (MTA)'s bridges and tunnels, issued a memo to request facial detection and recognition at all Triborough Bridge and Tunnel Authority facilities, stating,

---

189 Source: Waitt.

190 "Memo: New York Called for Face Recognition Cameras at Bridges, Tunnels," Vocativ, last modified January 27, 2017, http://www.vocativ.com/396745/memo-new-york-called-for-face-recognition-cameras-at-bridges-tunnels/.

> The Authority is interested in implementing a Facial Detection System, in a free-flow highway environment, where vehicle movement is unimpeded at highway speeds as well as bumper-to-bumper traffic, and license plate images are taken and matched to occupants of the vehicles (via license plate number) with Facial Detection and Recognition methods from a gantry based or road-side monitoring location.[191]

The MTA recently constructed towers to house homeland security equipment but would not reveal the capabilities of the towers—or whether the towers include FRT.[192] The integration of surveillance technologies, however, clearly illustrate that government agencies are evaluating various technologies to determine overall efficacy.

Drones can be enabled with FRT to identify persons on the ground for surveillance, search for specific individuals, and monitor such remote locations as large outdoor events.[193] These functions would significantly benefit law enforcement because drones can access densely populated events—in particular, New Year's Eve celebrations at Times Square in New York City—to scan crowds for suspicious persons at and near the event. BWCs outfitted with real-time FRT also have benefits despite the challenges and additional research needed to understand their long-term effects on society. In addition to personal safety, officers would have real-time information of persons with arrest warrants or individuals on FBI terror watch lists.

The NYPD equips each of its approximately 36,000 officers with a smartphone. Department phones give officers real-time data such as information on wanted persons, active warrants in multi-dwelling locations, the history of a location, 9–1-1 calls, ShotSpotter information, and many other functions. In a recent arrest, NYPD officers recovered two firearms and arrested three individuals after responding to a report of shots

---

[191] Lynn Gore, "Request for Information (RFI), RFI-16-63, All-Electronic Facial Detection and Recognition System at all TBTA Facilities" (official memorandum, MTA Bridges and Tunnels, December 12, 2016), https://www.documentcloud.org/documents/3428597-RFI.html.

[192] Andrew Siff, "New MTA Towers Can Read License Plates, and Maybe More," NBC (New York), September 28, 2017, http://www.nbcnewyork.com/news/local/MTA-Bridge-and-Tunnel-Gateway-Towers-Can-Read-License-Plates-Security--448568193.html.

[193] Hwai-Jung Hsu and Kuan-Ta Chen, "Face Recognition on Drones: Issues and Limitations" in *DroNet '15: Proceedings of the First Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use* (New York: ACM Press, 2015), 39, http://dl.acm.org/citation.cfm?doid=2750675.2750679.

being fired. Responding officers had used their smartphones to ascertain whether individuals with active warrants were at the location.[194] If the NYPD uses FRT on department smartphones, officers could ascertain the identity of individuals without identification by taking a photograph and using the picture to compare the person to those contained in a database.

C. CHALLENGES

Law enforcement anticipates several potential challenges in using FRT. The NYPD must address privacy, accuracy, and public trust of real-time FRT and gain public acceptance to adopt real-time FRT successfully as a viable law enforcement tool.

The ability of law enforcement to mitigate privacy concerns remains uncertain partially because no universal policies exist for collecting, sharing, and disseminating facial recognition data. A New York University study argues that law enforcement agencies should focus on the ethical issues raised with sharing data because expanding the use of new technologies compromises the desire of an individual to have complete and absolute privacy.[195] Although it is important for law enforcement agencies to focus on the moral and ethical concerns of citizens, it is vital to understand how citizens want to be policed.

Inaccuracy, blurred or partial images, intentional circumvention of facial recognition cameras, and other factors may affect the identification of wanted persons or persons of interest. Although FRT is increasingly more accurate than ever before, it is still imperfect, and as such, several variables will inevitably contribute to false positives, false negatives, and undetected faces. Technology company NEC has developed algorithms that utilize the "generalized matching face detection method," which "provides high speed and high accuracy for facial detection and facial features extraction."[196]

---

[194] "Finest Technology Helps New York's Finest Take Two Guns off the Streets," NYPD News, December 8, 2015, http://nypdnews.com/2015/12/finest-technology-helps-new-yorks-finest-take-two-gun-off-the-streets/.

[195] Lane et al., *Privacy, Big Data, and the Public Good*, 49.

[196] "Technology," NEC Corporation, accessed April 15, 2018, http://www.nec.com/en/global/solutions/safety/Technology/FaceRecognition/index.html.

Negative public perception epitomizes the challenges of real-time FRT and its use by law enforcement. Public trust of police has deteriorated in recent years and must be rebuilt to establish communities that work together with the police. Some potential community concerns over the use of real-time FRT are relevant in this discussion.[197] One specific concern expressed by citizens is that FRT will increase racial bias toward minorities when used by law enforcement. Although the FBI states in its report that FRT is not biased in any way—because it relies on existing data on criminals—the technology still identifies minorities, African Americans particularly, at a higher rate than other races.[198] Increased stops without probable cause to arrest may increase situations where police use force against minorities and worsen the fragile ecosystem of limited trust that has taken decades to build between law enforcement agencies and minority communities.

1. Privacy

Privacy is the leading concern for citizens involving surveillance technologies used by law enforcement. Nissenbaum and Introna contend that privacy is one of the "most prominent concerns raised by critics of FRT."[199] Real-time FRT can operate clandestinely, so the potential uncertainty surrounding its use of identifying information is unnerving for most citizens. Privacy, as defined by Ruth Gavison, is a "measure of the access others have to you through information, attention, and physical proximity."[200] Informational privacy, or control over personal information, is the principal concern involving FRT, due to a citizen's lack of control over personal information—and the wish to remain anonymous regardless of the technology's security benefits. The security and safety of the people,

---

[197] Trevor Kapp, "Neighborhood Policing Changing Attitudes and Reaping Benefits, NYPD Says," DNA Info, April 6, 2017, https://www.dnainfo.com/new-york/20170406/central-harlem/nypd-neighborhood-policing-nco-community-police-department.

[198] Nellie Bowles, "'I Think My Blackness Is Interfering': Does Facial Recognition Show Racial Bias?," *Guardian*, April 8, 2016, http://www.theguardian.com/technology/2016/apr/08/facial-recognition-technology-racial-bias-police.

[199] Lucas Introna and Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues* (New York: Center for Catastrophe Preparedness and Response, 2010), 44, https://www.nyu.edu/projects/nissenbaum/papers/facial_recognition_report.pdf.

[200] Ruth Gavison, "Privacy and the Limits of Law," *Yale Law Journal* 89, no. 3 (1980): 434–435, https://www.jstor.org/stable/pdf/795891.pdf.

however, remain the primary concern of law enforcement agencies, as they are part of every officer's sworn duty to serve and protect.

The definition of privacy is often conceptual with various meanings loosely based on Fourth Amendment rights. Norma Mollers and Jens Halterlein, who examine privacy issues in public discourse, contend, "In dealing with surveillance, scholars have widely agreed to refute privacy as an analytical concept. Nonetheless, in public debates, surveillance technologies are still confronted with issues of privacy, and therefore, endured as an empirical subject of research on surveillance."[201] Privacy will always be a topic of concern, especially because of the new paradigm shift toward technology-based policing.

Real-time FRT in the subway system moving more than six million people per day will analyze unprecedented amounts of information about citizens. Without specific laws governing law enforcement's use of FRT, many contend that databases will identify people at the whim of law enforcement and, as a result, violate the constitutional rights of citizens.[202] Some scholars argue that FRT will increase the likelihood of racial profiling and greater scrutiny among particular races, ethnicities, or religions. A New York University study suggests, "Historically affected racial groups will generate increased false positives based upon the methods in how certain systems identify individuals."[203] Because of these performance biases, individuals with prior negative interactions with police may see FRT as only another form of racial discrimination. The propensity for bias in policing has always been a topical concern, but with biometric technologies rapidly evolving and being used by law enforcement, state legislators are quickly trying to create new laws to

---

[201] Norma Möllers and Jens Hälterlein, "Privacy Issues in Public Discourse: The Case of 'Smart' CCTV in Germany," *Innovation: European Journal of Social Sciences* 26 (March 1, 2013): 65, https://publishup.uni-potsdam.de/opus4-ubp/frontdoor/deliver/index/docId/7767/file/moellers_diss.pdf#page=73.

[202] Kanya A. Bennett, "Can Facial Recognition Technology Be Used to Fight the New Way against Terrorism: Examining the Constitutionality of Facial Recognition Surveillance Systems," *North Carolina Journal of Law & Technology* 3 (2001): 151, http://ncjolt.org/can-facial-recognition-technology-be-used-to-fight-the-new-war-against-terrorism-examining-the-constitutionality-of-facial-recognition-surveillance-systems/.

[203] Introna and Nissenbaum, *Facial Recognition Technology*, 45.

build on the Illinois Biometric Act, which focuses on protecting individual privacy.[204] The goal of the new legislation is an attempt to keep pace with the rapid evolvement of biometric technology.

Technological advancements with facial recognition have outpaced legislation, and private organizations are utilizing FRT to perform a variety of functions—corporations large and small are creating personalized databases and developing new uses for the data, all with very few restrictions. Martin Abrams, president of the Centre for Information Policy Leadership at Hunton & Williams, states, "The nature of what we can capture about individuals is expanding faster than our ability to think about whether it's prudent to do so."[205] Author Muzamil Riffat explains,

> Although the notion of privacy as a right does not specifically appear in the U.S. constitution, it can be deduced from other related provisions. The amendments made to the Constitution afterward are understood to have addressed the concerns related to the protection of privacy. These are the First (speech, religion), Third (quartering soldiers), Fourth (against seizure and searches), Fifth (against self-incrimination), ninth (for general liberties) and fourteenth amendments (for personal liberty versus state action).[206]

The Fourth Amendment has the strongest role in determining loose guidelines for what is accepted as reasonable if FRT is used in public spaces.[207] The argument can be made, however, that public places diminish levels of privacy. Professor Peter Squire explains,

---

[204] Mark Melodia, Paul Bond, and Angela-Angelovska-Wilson, "Legal Risks and Rules of the Move to Biometrics," *New York Law Journal*, March 2, 2015, https://www.technologylawdispatch.com/wp-content/uploads/sites/26/2016/02/Legal-NYLJ-Article-Risks-and-Rules-of-the-Move-to-Biometrics.pdf.

[205] Melissa Maleske, "Facial Recognition Presents Privacy Concerns," Inside Counsel, March 2012, https://www.law.com/almID/4f46a3f8150ba0c00a000048/.

[206] Muzamil Riffat, "Legal Aspects of Privacy and Security: A Case- Study of Apple versus FBI Arguments," Sans Institute, June 1, 2016, 5, https://www.semanticscholar.org/paper/Legal-Aspects-of-Privacy-and-Security%3A-A-Case-Study/5f9139b8aa661bd040eec464d16ce31fbb829af5.

[207] Andrew H. Peterson, Jesse L. Kirkpatrick, and Deborah A. Boehm-Davis, *Developing Ethical, Legal, And Policy Analyses Relevant to the Use of Machine Learning Algorithms in National Security* (white paper, George Mason University, 2017), 2, http://sites.nationalacademies.org/cs/groups/dbassesite/documents/webpage/dbasse_179882.pdf.

"Some might argue that individuals consent to going outside or to other public places (i.e., a bank or mall) where security cameras are present."[208]

Federal laws address the use, collection, and storage of personal information. The Driver's Privacy Protection Act, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, the Fair Credit Reporting Act, and the Children's Online Privacy Protection Act all address personal information and were created to establish, maintain, and protect a person's right to privacy. These laws, however, have severe limitations addressing the recent methods of data collection through biometric technologies. No privacy laws exist that allow individuals to control the amount of information that can be digitally collected without their knowledge. In addition, law enforcement is not governed by a universal policy that would oversee the use of real-time FRT.

Politicians are just beginning to examine the impact of FRT and the ways it affects civil liberties and constitutional rights. The virtual absence of legislation or specific regulations pertaining to the public, private, or government use of FRT creates a dichotomy between law enforcement and citizens, in that trust of the police by citizens may weaken if FRT policies are created by law enforcement without oversight. New York State has enacted no laws pertaining to the specific use of FRT. The federal government, however, opted to examine the feasibility of developing a framework for FRT.

On March 22, 2017, the House committee on oversight and government reform established a subcommittee to review law enforcement's policies on FRT, with the intention of developing a framework for FRT, reviewing its benefits, challenges, and various uses, and determining whether legislation is necessary. The Center on Privacy and Technology at Georgetown Law estimated that, when accounting for all databases to which law enforcement has access, "one in two Americans is in a facial recognition network."[209] Law enforcement contends that a database of individuals can be beneficial whereas some

---

[208] Ms. Smith [pseud.], "You Consent to a Search If a Camera Sees You?: Facial Recognition vs. 4th Amendment," CSO, March 22, 2012, https://www.csoonline.com/article/2221971/microsoft-subnet/you-consent-to-a-search-if-a-camera-sees-you--facial-recognition-vs-4th-amendment.html.

[209] Garvie, Bedoya, and Frankle, *The Perpetual Line-Up*, 1.

citizens are distrustful of law enforcement's intentions of leveraging massive databases created by FRT. The FBI's Next Generation Identification System includes "an Interstate Photo System that allows the FBI and selected state and local law enforcement to search a database of over 30 million photos. The FBI also has agreements with at least 17 states that allow a request for a facial recognition search of state driver's license databases."[210] Privacy impact assessments for the Facial Analysis, Comparison, and Evaluation Services Unit—with the ability to compare facial images of persons associated with open assessments and active investigations—and the Next Generation Identification–Interstate Photo System—a mugshot repository—have been prepared by the FBI, approved by the Department of Justice, and posted on the public-facing website of the FBI.[211] Therefore, based on government actions, many public advocacy groups do not believe law enforcement can effectively keep such an expansive database completely confidential. While information sharing occurs between agencies, however, they are working to create a transparent environment, often documenting their policies online for public consumption.

While none of these best practices are mandated, certain guidelines reflect common-sense standards and can serve as a framework to limit liability for corporations and law enforcement agencies. The National Telecommunications & Information Administration has developed written guidelines for facial recognition implementers and software operators to determine the most appropriate way to proceed in an environment where law and policy have failed to keep pace.[212]

---

[210] Anil K. Jain, "Next Generation Biometrics" (presentation, Michigan State University, December 10, 2009), 10, http://biometrics.cse.msu.edu/Presentations/ Next_generation_biometrics_Korea_Dec2010.pdf.

[211] "Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit," Federal Bureau of Investigation, May 1, 2015, https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/facial-analysis-comparison-and-evaluation-face-services-unit.

[212] "Privacy Best Practice Recommendations for Commercial Facial Recognition Use," National Telecommunications and Information Administration, accessed March 28, 2018, https://www.ntia.doc.gov/ files/ntia/publications/ privacy_best_practices_recommendations_for_commercial_use_of_facial_recogntion.pdf.

a. Data Collection/Invasiveness

Some biometric technologies, such as fingerprint scans, are embraced by law enforcement more than other biometrics, such as FRT. Most biometric technologies gather information with the permission or at least the knowledge of the individual. FRT, however, can operate clandestinely and capture significant amounts of information on citizens. Real-time FRT, if used by law enforcement, can instantly identify anonymous individuals, and if FRT integrates with other databases, the flow of information can be unlimited. For example, other law enforcement databases—which contain LPR, summons, and arrest data, BWC footage, images from drones, integrated government databases, social media, open-source data, and employment information—can provide officers with geo-coded timelines. These can provide officers information containing both anecdotal and investigative value. This future examination illustrates how FRT can easily integrate with other technologies, demonstrates the capabilities of surveillance technologies, and therefore, reveals the necessary steps for protecting and safeguarding FRT data.

b. Misuse

Critics express significant concerns that law enforcement officers may intentionally misuse FRT for personal gain and inappropriately share confidential information. Real-time identification of strangers, including victims of stalking or domestic violence, if used for nefarious purposes, has chilling effects.[213] Similar to LPR technology scans when officers use state databases to conduct name checks, officers using FRT would be able to obtain personal data that if misused, may incur departmental and criminal sanctions.

In addition, critics raise concerns that law enforcement's use of FRT may cause racial bias toward minorities. Although the FBI states in its report that FRT does not augment existing data on criminals, it still identifies minorities, African Americans in particular, at higher rates than other races.[214] FRT can be used in law enforcement with any device equipped with a camera. BWCs, cell phones, fixed cameras, mobile cameras,

---

[213] Erica Klarreich, "Hello, My Name Is," *Communications of the ACM* 57, no. 8 (August 2014): 19, https://doi.org/10.1145/2632040.

[214] Lynch, *Face Off*, 2.

and even drone technology can be equipped with FRT software. The methodology behind law enforcement's FRT data collection, sharing, and duration of storage depends on policies created by each agency.

c. Ineffective Policies

Law enforcement organizations require transparency to ease tensions among citizens, and therefore, when government agencies use surveillance technologies, it is imperative to be as transparent as possible. Sabrina A. Lochner contends the use of FRT is a serious concern if law enforcement agencies fail to inform citizens of its use.[215] Her 2012 article raises policy and privacy questions about mobile FRT and iris scans used by law enforcement. By not making citizens aware that their personal information is being captured, law enforcement and the private sector are putting public trust and transparency at risk.

Another challenge for law enforcement lies in creating and establishing comprehensive mechanisms to prevent officer misuse of FRT. As discussed previously, the Metropolitan Police used real-time facial recognition during a November 2017 remembrance ceremony attended by 10,000 people. The department compared the faces of individuals in the crowd to a database of approximately 50 individuals known to exhibit dangerous behavior to public officials.[216] Martha Spurrier, director of advocacy group Liberty, states, "There is no legal basis and no public consent for deploying this intrusive and intimidating biometric surveillance in public space."[217] American critics of FRT contend that it will be similarly misused by U.S. police departments. The ACLU has shown concern that BWCs—equipment for which the organization previously advocated to increase police accountability—will be used as surveillance machines once integrated with FRT. Cultural barriers to FRT, specifically its use by law enforcement, need to be

---

[215] Sabrina A Lochner, "Saving Face: Regulating Law Enforcement's Use of Mobile Facial Recognition Technology & Iris Scans," *Arizona Law Review* 55 (2013): 33, 202, http://www.arizonalawreview.org/pdf/55-1/55arizlrev201.pdf.

[216] Townsend, "Police to Use Facial-Recognition Cameras."

[217] Townsend.

addressed by examining other law enforcement technologies that are also imperfect, to mitigate citizen privacy concerns.

Concerns over lack of transparency are not only aired in the public sector but in the private sector as well. Facebook could be fined billions of dollars due to its facial recognition application, which according to a class action lawsuit, violates the Illinois Biometric Information Privacy Act.[218] Judge Donato ruled that the Illinois law is clear and that Facebook collected a "wealth of data on its users, including self-reported residency and IP addresses."[219]

d. Data Storage, Data Sharing, and Hacking

With the evolution of cloud technology and the ability to store large amounts of data, law enforcement organizations are challenged with risks to stored information that may be compromised. Each piece of collected information, if compromised, may be used nefariously. Government databases are often the biggest target for hackers, facing daily cyber threats that are unique because of potential harm that stolen information inflicts on citizens. For example, the 2014 breach at the U.S. Office of Personnel Management (OPM), in which 22 million personnel records containing personal data—work history, family members' names, fingerprints, and personal references—were compromised.[220] Incidents such as the OPM hacking serve as examples of how public trust in the government erodes when a database, law enforcement or otherwise, falls prey to a security breach.

Many civil liberty groups criticize biometric data storage and data sharing. The ACLU urges "caution in its [biometric technology's] deployment and stringent safeguards in its use.[221] Use of biometrics, however, has helped the Australian Government

---

[218] Lucas Nolan, "Facebook Could Face Billions in Fines over Facial Recognition Features," Breitbart, April 17, 2018, http://www.breitbart.com/tech/2018/04/17/facebook-could-face-billions-in-fines-over-facial-recognition-features/.

[219] Nolan.

[220] Eggers, *Delivering on Digital*, loc. 2957.

[221] "Biometrics," American Civil Liberties Union, accessed July 6, 2018, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/biometrics.

Department of Immigration and Border Protection combat identity fraud. The international information-sharing agreements between other countries, which involve the sharing of facial images, allow each country to track biographical data, copies of immigration documents, immigration status, and criminal history relevant to immigration purposes.

2. Accuracy

The NYPD will need to address accuracy concerns associated with the use of real-time FRT, even though imperfections exist and are expected to occur with any technology. Joy Buolamwini expresses concerns about disparities in FRT's ability to identify races and gender successfully.[222] Buolamwini examined the programming used in facial recognition and concluded that machine-learning algorithms have difficulties in identifying and even discriminate against certain races as well as gender. Her study examined three commercial facial recognition systems and determined that darker-skinned females were most often misclassified (34.7 percent of the time) whereas the error rate for light-skinned males was 0.8 percent. Based on Buolamwini's research, someone may be wrongfully accused of a crime based on erroneous yet confident misidentification of the perpetrator from security video footage analysis.

Further adding to reliability concerns, specifically in how results may affect court verdicts, is the problem of FRT encountering identical twins. A 2011 study contends that FRT can identify identical twins with 90 percent accuracy.[223] More recent studies recommend further research to determine the true scope of FRT's ability to differentiate between identical twins.[224] Apple, regarding its FaceID software, acknowledges that the statistical probability is "different" for twins than for random persons, which has an

---

[222] Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research* 21 (2018): 1–2, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[223] P. Jonathan Phillips et al., "Distinguishing Identical Twins by Face Recognition," in *Face and Gesture* (Piscataway, NJ: IEEE, 2011), 185–187, https://doi.org/10.1109/FG.2011.5771395.

[224] Raghavendra Ramachandra and Christoph Busch, "Presentation Attack Detection Methods for Face Recognition Systems: A Comprehensive Survey," *ACM Computing Surveys* 50, no. 1 (March 20, 2017): 29, https://doi.org/10.1145/3038924.

accuracy rate of 99.997 percent.[225] An inaccurate FRT system may lead to persons being unnecessarily stopped by police and, thus, imposes the onus of proving one's identity.

a. False Positives and False Negatives

Although FRT has experienced significant improvements and is more accurate than ever before, false positives and false negatives still occur. A false positive occurs when FRT incorrectly matches an individual to a person contained in the database.[226] Conversely, a false negative occurs when an individual is not matched, but the individual should have been identified by the image contained within the system.[227] While false negatives pose an unnecessary safety risk to citizens, false positives damage police relations with the communities they serve. Stopping individuals positively identified by facial recognition systems in crowded New York City subway stations due to false positive matches can have damaging effects on the NYPD. In addition, the potential exists for increased civilian complaints against officers, as well as the potential for adversarial interactions between citizens and the police.

b. Intentional Circumvention

The potential exists for certain individuals to evade FRT cameras. Since the inception of CCTV, those who wish to elude identification do so by simply avoiding the cameras or covering their faces. With FRT, covering a portion of the face, wearing sunglasses or masks, or using cosmetics to change appearance will more than likely circumvent FRT. But as real-time FRT evolves and deep-learning neural networks continue to advance, sunglasses and partial face covering may not outwit facial recognition software in the future.

To further complicate the technological challenges of FRT, companies are spawning new ideas to protect individual anonymity. Technologist Adam Harvey created

---

[225] "About Face ID Advanced Technology," Apple Support, accessed April 21, 2018, https://support.apple.com/en-us/HT208108.

[226] Lynch, *Face Off*, 6.

[227] Lynch, 6.

a clothing line that has coded patterns designed to look fashionable, but images disguised within the pattern confuse FRT systems and create thousands of false negatives because current real-time facial recognition systems are unable to discern which images are real.[228]

3. Transparency and Public Trust

Public support of the NYPD has transformed in recent years given the department's focus on neighborhood policing and strong police–community relations. The introduction and acceptance of new surveillance technologies, however, may bring substantial criticism that overshadows those supportive of real-time FRT.

Public trust remains a challenge for law enforcement. In addition, law enforcement agencies wishing to pursue FRT will face additional hurdles. Matt Wood, general manager of artificial intelligence at Amazon Web Services, points out that Amazon's FRT has benefited society through law enforcement's use in preventing human trafficking, inhibiting child exploitation, and reuniting missing children with their families. Wood suggests there are positives and negatives with any new technology, but imposing a ban—such as the one requested by other Amazon employees for the sale of FRT to law enforcement—is short sighted. Society simply needs to ensure that this technology is used the right way.[229]

a. Transparency

Law enforcement organizations looking to become more transparent have prioritized technologies that address community relations, such as BWCs, over other technologies, regardless of their documented success in fighting crime or combating terrorism. This is evident in the tremendous cost of BWC initiatives undertaken by law enforcement agencies around the world. In 2016, President Obama allocated $263 million

---

[228] Alex Hern, "Anti-Surveillance Clothing Aims to Hide Wearers from Facial Recognition," *Guardian*, January 4, 2017, http://www.theguardian.com/technology/2017/jan/04/anti-surveillance-clothing-facial-recognition-hyperface.

[229] Matt Wood, "Some Quick Thoughts on the Public Discussion Regarding Facial Recognition and Amazon Rekognition This Past Week," *AWS New Blog*, June 1, 2018, https://aws.amazon.com/blogs/aws/some-quick-thoughts-on-the-public-discussion-regarding-facial-recognition-and-amazon-rekognition-this-past-week/.

to fund 50,000 BWCs across the United States, based on his belief that more transparency between law enforcement and citizens is needed.[230] As a result, questions and concerns of law enforcement transparency for surveillance technologies, such as LPRs and FRT, are not the primary focus for advocacy groups and those critical of law enforcement tactics and strategies. In recent years, officer use-of-force encounters and police transparency have garnered strong scrutiny in the wake of several high-profile incidents involving police and citizens.

b. Community Mistrust of Police

Employees of major technology companies criticize company policies that allow sharing of FRT with law enforcement. On June 21, 2018, more than 100 Amazon workers signed and sent a letter to CEO Jeff Bezos asking the company to stop selling facial recognition software to law enforcement.[231] The letter revealed their distrust of the police, stating that this technology would "ultimately harm the most marginalized" based on law enforcement's "historic militarization of police, renewed targeting of Black activists, and the growth of a federal deportation force currently engaged in human rights abuses."[232] This letter came after the ACLU reported on Amazon providing facial recognition software to law enforcement.

Citizens have different perspectives when asked about how law enforcement uses LPR technology, BWCs, and FRT. All share similar opinions on accuracy, reliability, and use, which can substantially affect police relations with the community. FRT, however, is culturally perceived by critics as a technology that will do more harm than good, when used by law enforcement. Therefore, the NYPD's use of real-time FRT may initially experience mixed reactions from community members.

---

[230] Mark Landler, "Obama Offers New Standards on Police Gear in Wake of Ferguson Protests," *New York Times*, December 1, 2014, https://www.nytimes.com/2014/12/02/us/politics/obama-to-toughen-standards-on-police-use-of-military-gear.html.

[231] Greg Sandoval, "Over 100 Amazon Employees, Including Senior Software Engineers, Signed a Letter Asking Jeff Bezos to Stop Selling Facial-Recognition Software to Police," *Business Insider*, June 22, 2018, http://www.businessinsider.com/over-100-amazon-employees-sign-letter-jeff-bezos-stop-selling-facial-recognition-software-police-2018-6.

[232] Sandoval.

D. CONCLUSION

FRT, specifically its use in real time, serves a public benefit for citizens as well as personal, corporate, and law enforcement use. FRT's benefits to law enforcement are similar to those of LPR technology as long as law enforcement and government organizations create effective policies and ethical guidelines that govern its use. Significant public benefits exist in the form of safer streets, and even if the probability of identifying a known terrorist through real-time FRT turns out to be small, evidence shows that in a controlled environment, such as the New York City subway system, this software is likely to be successful. Additionally, the NYPD is responsible for preventing violent acts. Real-time FRT could become an additional investigative tool that prevents further violence. For example, in June 2018, police identified Jerrod Ramos using FRT after he walked into the Capital Gazette in Maryland and killed five journalists.[233] The suspect was highly uncooperative, and police needed an immediate identification to ensure no additional threats existed.

Although little research has examined the results and effectiveness of real-time FRT for law enforcement, direct comparisons to LPRs illustrate the similarities of benefits and challenges in both technologies. In addition, both technologies have experienced significant advancements yielding additional benefits and new challenges, which have been identified by both advocacy groups and citizens. It is possible that FRT will show similar successes and public acceptance to those of LPR technology if law enforcement closely applies the lessons learned during LPR implementation.

[233] Cade Metz and Natasha Singer, "Newspaper Shooting Shows Widening Use of Facial Recognition by Authorities," *New York Times*, July 1, 2018, https://www.nytimes.com/2018/06/29/business/newspaper-shooting-facial-recognition.html.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CONCLUSION

> *The United States is better organized and equipped to combat terrorism, but its citizens remain fearful. The United States' frightened, angry, and divided society remains the country's biggest vulnerability.*
>
> —Brian Jenkins, "Where Are We in the 'War on Terror?"[234]

Overall, this thesis concludes that, while decision-makers must mitigate challenges to receive public support, real-time FRT is not nearly as frightening as it might seem to some. In other words, having compared it to LPR technology, this thesis lays out the tools law enforcement leaders already have to mitigate the fears, particularly in connection with well-established policies and practices that protect civil liberties. Once law enforcement mitigates the challenges of FRT, the benefits will surely outweigh them. Law enforcement use of FRT must be ethical, transparent, and responsible. Other places, such as China, have different visions of its intended use, which do not conform to the values and privacy considerations upheld by the NYPD. This chapter concludes the thesis by reviewing the fundamental challenges and benefits identified with LPRs as well as the lessons learned from BWCs, so the NYPD can apply them in evaluating real-time FRT. The chapter ends with thoughts on why the NYPD should mitigate the challenges and gain public support, so the community as a whole may benefit from the real-time use of FRT.

LPR technology is not a panacea for solving all crimes, countering all terrorist actions, or finding every lost child, but LPRs provide law enforcement with significant benefits. Additionally, LPRs can be integrated with other law enforcement technologies. The capabilities of LPR technology have recently expanded, with new uses for both law enforcement and the private sector, despite the concerns identified in this thesis. Benefits relating to crime prevention illustrate the growing trend in which LPR technology uses new methods to enforce the laws, such as red light and speed cameras to enforce traffic codes.

---

[234] Brian M. Jenkins, "Fifteen Years on, Where Are We in the 'War on Terror?,'" Combating Terrorism Center, September 7, 2016, https://ctc.usma.edu/fifteen-years-on-where-are-we-in-the-war-on-terror/.

The expansion of LPR technology in New York City demonstrates that citizens are not overtly opposed to its use.

The NYPD has developed sound policies regarding LPRs and already mitigated many of the challenges to minimize potential harm to civil liberties and misuse. In addition, LPRs are generally accepted as a common law enforcement technology, largely in part because the NYPD previously addressed many of the risks. The NYPD addressed LPR data collection, retention, and sharing through robust and clear policies. In addition, the department addressed potential misuse of LPRs to eliminate the ambiguities and clearly define acceptable practices. The NYPD can apply the same strategies to address the challenges with FRT because both technologies perform similar functions. FRT and LPRs are alike in that both technologies collect all available information, without bias, from license plates or persons. Furthermore, both technologies use hot lists to compare against collected data, and the information received requires human intervention to verify the information, such as a stolen vehicle or a wanted person.

A police officer with a sharp eye can detect a stolen vehicle from information contained in a police report, which is similar to a police officer recognizing the face of an individual wanted for a previous crime. LPRs and real-time FRT both act as force multipliers for police officers on the street by scanning vehicles and persons. In New York City, a police officer could not possibly do all the work that technology can do, and therefore, technology can assist yet not replace police officers. In the NYPD, public acceptance of LPR exists because many of the challenges have been addressed. Therefore, the NYPD can apply a similar framework to real-time FRT whereby the department already addressed LPRs.

The NYPD should consider real-time FRT to help facilitate greater efficiencies in policing and to work in conjunction with other technologies and law enforcement tools. In addition, real-time FRT can be used by the NYPD as another tool for police officers in the field. For example, NYPD police officers carry many less-lethal devices—pepper spray, conducted electrical devices, and impact weapons—so if one tool is ineffective in a given situation, officers have other options to mitigate a potential threat. Real-time FRT can be

used alongside other technologies and equipment to enhance public safety and maintain law and order.

Further research will be necessary to determine the overall effectiveness of actual real-time FRT. The benefits of integrating real-time FRT with other technology platforms, such as smartphones and BWCs, could be immeasurable. The challenges, however, must be carefully managed to successfully implement a system that garners public acceptance by the majority. Overall, negative connotations surrounding the use of real-time FRT, specifically when used by law enforcement, have emerged because the public benefit has not yet been established. With LPRs, documented evidence shows their benefit as a force multiplier in reducing crime, aiding in investigations, conducting summons enforcement, easing traffic congestion, allowing toll payments, and identifying missing persons, wanted felons, and potential terrorists. The challenges faced by law enforcement—privacy concerns, officer misuse, inaccuracy, lack of transparency, as well as the methods by which data is collected, stored, and shared—are not entirely solved, but in New York City, current policies and procedures ease many of the concerns and show that citizens are not strongly opposed to the use of LPR technology. The benefits and challenges of LPRs, FRT, and BWCs for law enforcement are enumerated in Tables 1 and 2, respectively.

Table 1. Comparison of Benefits of LPRs, FRT, and BWCs

	Facial Recognition Technology	**License Plate Readers**	**Body-Worn Cameras**
Crime Prevention	Effective; Encompasses Crowded Environments	Effective in Targeted Areas	Effective in the Wearer's Peripheral Vision, Surroundings
Investigating Terrorism	Precautionary Measures	Remedial Measures	Uncorrelated
Real-Time IDs of Wanted/Known	Instant ID of Individuals	Instant ID of Plate Numbers	Instant Record of Wearer's Peripheral Vision, Surroundings
Investigative Assistance	Effective; Easy to Detect Suspects, Wanted Persons	Effective; Easy to Detect Vehicle History	Effective in Officer Assessments and Engagements
Officer Safety	Uncorrelated, Unless Integrated with Other Tech	Unbiased Policing; Increased Awareness; Safe Driving	Mindful of One's Actions
Mental Health Support	Instant ID of Person; Emergency, Special Needs Info	Instant IDs of Vehicle Owner's License, Health Conditions	Within Wearer's Ability
Missing Persons	Instant ID of Individual's Location	Amber Alerts, However, Limited	Within Wearer's Ability
Overcrowding in Transit	Eliminates Turnstiles; Utilizes EZ-Pass Method for Transit	Uncorrelated	Uncorrelated
Integration with Other Tech	Versatile	Limited	Limited

Table 2. Comparison of Challenges with LPRs, FRT, and BWCs

	Facial Recognition Technology	**License Plate Readers**	**Body-Worn Cameras**
Privacy: Data Collection; Invasiveness	Continuous Data Collection of Citizen's Personal Info	Stores Vehicle Records Regardless of Illicit Activity	Video Footage Recorded at the Discretion of Wearer
Privacy: Misuse	Personal Records Can Be Abused; May Cause Racial Bias	Abuse of Vehicular Activity; Selective Enforcement	Camera Can Be Deactivated during Unfavorable Situation
Privacy: Ineffective Policies	Difficult to Create, Establish Comprehensive Mechanisms to Prevent Officer Misuse	Policies Vary by Agency	Inconsistent Policies within Each Department
Privacy: Data Storage, Sharing, Hacking	Risk of Personal Data Being Compromised by Hackers	Requires Abundant Storage Space; Risk of Cyber Attacks	Requires Abundant Storage Space; Risk of Video Being Compromised by Hackers
Accuracy: False Positives; False Negatives	Unnecessary Safety Risks; Damage to Police Relations	Difficulties Distinguishing between Identical Plates from Different States	Uncorrelated
Accuracy: Intentional Circumvention	Can Avoid Cameras or Cover Portions of the Face	LPR Signals Can Be Disrupted	Camera Can Be Deactivated
Transparency	Tech Addressing Community Relations Is Prioritized	Tech Addressing Community Relations Is Prioritized	Decision to Activate Camera Based on Department Policy, Transparency, Individual Privacy
Public Mistrust of Police	Distrust of Police Using Tech to Harm Marginalized Groups	Connections of Vehicle History to That of Illicit Behavior	Footage of Misconduct Raise Questions and Distrust

Technology is part of a crucial conversation in policy now. For example, BWCs were seen as an effective response in holding police accountable for use-of-force encounters as well as providing transparency in policing. The result of their use, however, created controversies between law enforcement and citizens due to inconsistent policies from one police department to another. BWCs were supposed to remove the ambiguity of policing and create an environment where policing is transparent, fosters stronger relations

between police and community, and decreases civilian complaints against police officers as well as use-of-force incidents. Instead, BWCs created a new level of privacy concerns; those concerns, however, are distinct from both LPRs and FRT. Officers use BWCs in most police interactions, often recording inside private residences and potentially capturing moments that citizens do not want memorialized on video. LPRs and FRT, on the other hand, record already public information—license plates and faces.

Law enforcement organizations, looking to become more transparent, have prioritized BWC implementation over other technologies to address community relations. U.S. law enforcement and legislators equally support the use of BWCs, but they fear law enforcement's use of real-time FRT will send the message that citizen privacy has been compromised, which is simply not a valid concern. This thesis concludes that the expectation of privacy inside a private residence greatly differs from privacy expectations in a public setting.

To address public trust concerns and create a model that fosters transparency, the NYPD initiated a robust strategy to rebrand the NYPD image. The strategy behind neighborhood policing facilitates collaboration between local police officers and members of the community to share the responsibility of safety in New York City neighborhoods, allowing communities to work in partnership with the NYPD. Neighborhood policing, combined with Build the Block meetings, facilitates conversations and answers questions about various surveillance technologies, including ideas from citizens about how communities want to be policed. The NYPD must continue to take proactive steps, using neighborhood policing as a platform for better community relations, transparency, and the opportunity for citizens to understand how the NYPD can and will use real-time FRT. Once the NYPD garners public acceptance, it may realize the use of real-time FRT for a safer New York City subway system.

LIST OF REFERENCES

Allevate. “Helping to Counter the Terrorist Threat Using Face Recognition.” July 28, 2017. http://allevate.com/index.php/2017/07/28/helping_to_counter_the_terrorist_threat_using_face_recognition/.

American Civil Liberties Union. “Biometrics.” Accessed July 6, 2018. https://www.aclu.org/issues/privacy-technology/surveillance-technologies/biometrics.

Anderson, Lisa. “Exclusive-Poll: New York City Transport Seen as Safest in World for Women.” Reuters. October 28, 2014. https://uk.reuters.com/article/women-poll-newyork/exclusive-poll-new-york-city-transport-seen-as-safest-in-world-for-women-idUKL6N0SB4WI20141029.

Apple Support. “About Face ID Advanced Technology.” Accessed April 21, 2018. https://support.apple.com/en-us/HT208108.

Baker, Al. “License Plate Cameras Aid in Police Investigations.” *New York Times*, April 11, 2011. https://www.nytimes.com/2011/04/12/nyregion/12plates.html.

———. “Street Stops by New York City Police Have Plummeted.” *New York Times*, May 30, 2017. https://www.nytimes.com/2017/05/30/nyregion/nypd-stop-and-frisk.html.

Bennett, Kanya A. “Can Facial Recognition Technology Be Used to Fight the New Way against Terrorism: Examining the Constitutionality of Facial Recognition Surveillance Systems.” *North Carolina Journal of Law & Technology* 3 (2001): 151–174. http://ncjolt.org/can-facial-recognition-technology-be-used-to-fight-the-new-war-against-terrorism-examining-the-constitutionality-of-facial-recognition-surveillance-systems/.

Bignami, Francesca, and Giorgio Resta. *Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance*. Rochester, NY: Social Science Research Network, 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3043771.

Biometrica Systems. “Biometrica Announces Release of New SSIN, with Mobile App That Allows Near Real-Time Facial Recognition.” November 23, 2016. https://biometrica.com/biometrica-announces-release-of-new-ssin-with-mobile-app-that-allows-near-real-time-facial-recognition/.

Bledsoe, Woodrow Wilson. *Proposal for a Study to Determine the Feasibility of a Simplified Facial Recognition Machine*. Palo Alto, CA: Panoramic Research, January 30, 1963. http://archive.org/details/firstfacialrecognitionresearch.

Bowles, Nellie. "'I Think My Blackness Is Interfering': Does Facial Recognition Show Racial Bias?" *Guardian*, April 8, 2016. http://www.theguardian.com/technology/2016/apr/08/facial-recognition-technology-racial-bias-police.

Brown, Steven Rex. "NYPD Ripped for Abusing Facial-Recognition Tool." *New York Daily News*, March 1, 2018. http://www.nydailynews.com/new-york/nyc-crime/nypd-ripped-abusing-facial-recognition-tool-article-1.3847796.

Buolamwini, Joy, and Timnit Gebru. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." *Proceedings of Machine Learning Research* 21 (2018): 1–15. http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

Byrne, John. "Emanuel Raises Facial Recognition Tech in Taxi vs. Ride-Share Debate." *Chicago Tribune*, November 7, 2017. http://www.chicagotribune.com/news/local/politics/ct-met-rahm-emanuel-rideshare-report-20171107-story.html.

Cavadini, Daniele, Andreas Meier, Daniel Fasel, and Lorenzo Cimasoni. "Introducing the Biometrical Electronic Passport (EPass)." Seminar, University of Fribourg, 2008.

City of New York. "Vision Zero: Mayor de Blasio Pushes for Tougher State Laws to Keep Dangerous Drivers off the Streets." March 15, 2018. https://www1.nyc.gov/office-of-the-mayor/news/136-18/vision-zero-mayor-de-blasio-pushes-tougher-state-laws-keep-dangerous-drivers-off-streets#/0.

City of New York, Police Department Legal Bureau. "Freedom of Information Law Request: #14-PL-0175." Letter to Nate Vogel, New York Civil Liberties Union, April 17, 2014. https://www.nyclu.org/sites/default/files/20140417_NYPDDenial_NYCLUFOILRequest.pdf.

Communities United for Police Reform. "Know Your Rights! Help End Discriminatory, Abusive & Illegal Policing!" Accessed May 6, 2018. http://changethenypd.org/resources/know-your-rights-help-end-discriminatory-abusive-illegal-policing.

Constitution Project. "Law Enforcement Facial Recognition Is a Powerful Surveillance Technology in Need of Independent Checks and Limits." March 30, 2017. https://constitutionproject.org/wp-content/uploads/2017/03/Facial-Recognition-Statement-for-Record_The-Constitution-Project.pdf.

Counter Extremism Project. "Vehicles as Weapons of Terror." May 22, 2017. https://www.counterextremism.com/vehicles-as-weapons-of-terror.

Crump, Catherine. "An Ethical Framework for Face Recognition." American Civil Liberties Union. July 16, 2013. https://www.ntia.doc.gov/files/ntia/publications/aclu_an_ethical_framework_for_face_recognition.pdf.

———. *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements*. New York: American Civil Liberties Union, July 2013. https://www.aclu.org/issues/privacy-technology/location-tracking/you-are-being-tracked.

Cuador, Claudia. "From Street Photography to Face Recognition: Distinguishing between the Right to Be Seen and the Right to Be Recognized." *Nova Law Review* 41, no. 2 (2017): 1–28. https://nsuworks.nova.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=1998&context=nlr/.

Customs and Border Protection. "CBP Deploys Facial Recognition Biometric Technology at 1 TSA Checkpoint at JFK Airport." October 11, 2017. https://www.cbp.gov/newsroom/national-media-release/cbp-deploys-facial-recognition-biometric-technology-1-tsa-checkpoint.

Daniel, Stephanie, Nicole Lewis, and Kalalea Kalalea. "In the Wake of Broken Windows Policing How Aggressive Policing Contributed to East Harlem Residents Distrust of Police." Master's capstone, City University of New York, 2016.

Davis, Wendy. "Facial Recognition Technology Nab Criminals-and Raises Privacy Concerns." ABA Journal. October 2017. http://www.abajournal.com/magazine/article/facial_recognition_technology_crime_privacy.

Dees, Tim. "Finding Stolen Vehicles." Hendon Media Group. Accessed June 3, 2018. http://www.hendonpub.com/resources/article_archive/results/details?id=3901.

Del Greco, Kimberly J. "Law Enforcement's Use of Facial Recognition Technology." Federal Bureau of Investigations. March 22, 2017. https://www.fbi.gov/news/testimony/law-enforcements-use-of-facial-recognition-technology.

Department of Homeland Security. "Privacy Impact Assessment for the Automated Biometric Identification System (IDENT)." Accessed August 8, 2018. https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-identappendices-august2017.pdf.

Deshmukh, Shubhada, Manasi Patwardhan, and Anjali Mahajan. "Survey on Real-Time Facial Expression Recognition Techniques." *IET Biometrics* 5, no. 3 (September 2016): 155–163.

Detsing, Jeerawat, and Mahasak Ketcham. "Detection and Facial Recognition for Investigation." In *International Conference on Digital Arts, Media and Technology*, 407–411. Piscataway, NJ: IEEE, 2017. https://doi.org/10.1109/ICDAMT.2017.7905002.

Dodd, Vikram. "Met Police to Use Facial Recognition Software at Notting Hill Carnival." *Guardian*, August 5, 2017. http://www.theguardian.com/uk-news/2017/aug/05/met-police-facial-recognition-software-notting-hill-carnival.

Doubek, James. “Digital License Plates Roll Out in California.” NPR. June 1, 2018. https://www.npr.org/sections/thetwo-way/2018/06/01/616043976/digital-license-plates-roll-out-in-california.

Drover, Paul, and Barak Ariel. “Leading an Experiment in Police Body-Worn Video Cameras.” *International Criminal Justice Review* 25, no. 1 (March 1, 2015): 80–97. https://doi.org/10.1177/1057567715574374.

Du, Shan, M. Ibrahim, M. Shehata, and W. Badawy. “Automatic License Plate Recognition: A State-of-the-Art Review.” *IEEE Transactions on Circuits and Systems for Video Technology* 23, no. 2 (February 2013): 311–325. https://doi.org/10.1109/TCSVT.2012.2203741.

Eggers, William D. *Delivering on Digital: The Innovators and Technologies That Are Transforming Government*. 1st ed. New York: Rosetta Books, 2016.

Eisler, Ben. “ACLU Concerned Automatic License Plate Readers May Invade Privacy.” WJLA News. July 30, 2012. http://wjla.com/news/local/aclu-concerned-red-light-cameras-may-invade-privacy-78301.

Federal Bureau of Investigation. “2015 Crime in the United States.” Accessed June 3, 2018. https://ucr.fbi.gov/crime-in-the-u.s/2015/crime-in-the-u.s.-2015/tables/table-1.

———. “2017 NCIC Missing Person and Unidentified Person Statistics.” Accessed June 17, 2018. https://www.fbi.gov/file-repository/2017-ncic-missing-person-and-unidentified-person-statistics.pdf/view.

———. “Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit.” May 1, 2015. https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/facial-analysis-comparison-and-evaluation-face-services-unit.

Find Biometrics. “Facial Recognition.” Accessed August 7, 2018. https://findbiometrics.com/solutions/facial-recognition/.

Fitzsimmons, Emma G. “Every New York City Subway Line Is Getting Worse. Here’s Why.” *New York Times*, June 28, 2017. https://www.nytimes.com/interactive/2017/06/28/nyregion/subway-delays-overcrowding.html.

Fortune. “Full Transcript of Hillary Clinton’s NAACP Speech: ‘This Madness Has to Stop.’” July 18, 2016. http://fortune.com/2016/07/18/hillary-clinton-speech-naacp-transcript/.

Francescani, Chris. “NYPD Expands Surveillance Net to Fight Crime as well as Terrorism.” Reuters. June 21, 2013. https://www.reuters.com/article/usa-ny-surveillance/nypd-expands-surveillance-net-to-fight-crime-as-well-as-terrorism-idUSL2N0EV0D220130621.

Future of Privacy Forum. *Privacy Principles for Facial Recognition Technology*. Washington, DC: Future of Privacy Forum, December 2015. https://fpf.org/wp-content/uploads/2015/12/Dec9Working-Paper-FacialRecognitionPrivacyPrinciples-For-Web.pdf.

Garvie, Clare, Alvaro Bedoya, and Johnathan Frankle. *The Perpetual Line-Up: Unregulated Police Face Recognition in America*. Washington, DC: Center on Privacy and Technology, Georgetown Law, October 18, 2016. https://www.perpetuallineup.org.

Gates, Kelly. “Identifying the 9/11 ‘Faces of Terror.’” *Cultural Studies* 20, no. 4/5 (September 7, 2006): 417–440. https://doi.org/10.1080/09502380600708820.

Gavison, Ruth. “Privacy and the Limits of Law.” *Yale Law Journal* 89, no. 3 (1980): 421–471. https://www.jstor.org/stable/pdf/795891.pdf.

Gierlack, Keith, Shara Williams, Tom LaTourrette, James M. Anderson, Lauren A. Mayer, and Johanna Zmud. *License Plate Readers for Law Enforcement: Opportunities and Obstacles*. Santa Monica, CA: RAND Corporation, 2014. https://www.rand.org/pubs/research_reports/RR467.html.

Goodman, J. David. “Court-Appointed Police Monitor Has Fought for City and against It.” *New York Times*, August 13, 2013. https://www.nytimes.com/2013/08/14/nyregion/court-appointed-police-monitor-has-fought-for-city-and-against-it.html.

Goodman, J. David, and Al Baker. “Police Shoot Hammer-Wielding Man Sought in 4 Manhattan Attacks.” *New York Times*, May 13, 2015. https://www.nytimes.com/2015/05/14/nyregion/officer-shoots-man-in-midtown-manhattan.html.

Gore, Lynn. “Request for Information (RFI), RFI-16-63, All-Electronic Facial Detection and Recognition System at all TBTA Facilities.” Official memorandum, MTA Bridges and Tunnels, December 12, 2016. https://www.documentcloud.org/documents/3428597-RFI.html.

Government Accountability Office. *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law*. GAO-15-621. Washington, DC: GAO, July 2015.

Griffin, Joel. “LPR Technology Comes of Age.” Security Info Watch. August 4, 2015. http://www.securityinfowatch.com/article/12099279/lpr-technology-comes-of-age.

Guzzardo, Jamie, and Jesse Solomon. “Missing Boy Spent 11 Days Wandering New York Subways.” CNN. November 25, 2009. http://www.cnn.com/2009/US/11/25/new.york.subway.teen/index.html.

Haigney, Sophie. “ACLU Sues Immigration and Customs Enforcement for License Plate Reader Records.” SF Gate. May 28, 2018. https://www.sfgate.com/bayarea/article/ACLU-sues-ICE-for-license-plate-reader-contracts-12937712.php.

Hern, Alex. “Anti-Surveillance Clothing Aims to Hide Wearers from Facial Recognition.” *Guardian*, January 4, 2017. http://www.theguardian.com/technology/2017/jan/04/anti-surveillance-clothing-facial-recognition-hyperface.

Higginbotham, Stacy. “Facial Recognition Freak Out: What the Technology Can and Can’t Do.” *Fortune*, June 23, 2015. http://fortune.com/2015/06/23/facial-recognition-freak-out/.

Hirose, Mariko. “Documents Uncover NYPD’s Vast License Plate Reader Database.” American Civil Liberties Union. January 25, 2016. https://www.aclu.org/blog/privacy-technology/location-tracking/documents-uncover-nypds-vast-license-plate-reader-database.

Hsu, Hwai-Jung, and Kuan-Ta Chen. “Face Recognition on Drones: Issues and Limitations.” In *DroNet ‘15: Proceedings of the First Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use*, 39–44. New York: ACM Press, 2015. http://dl.acm.org/citation.cfm?doid=2750675.2750679.

Huggler, Justin. “Facial Recognition Software to Catch Terrorists Being Tested at Berlin Station.” *Telegraph*, August 2, 2017. http://www.telegraph.co.uk/news/2017/08/02/facial-recognition-software-catch-terrorists-tested-berlin-station/.

INTERPOL. “Forensics.” Accessed July 3, 2018. https://www.interpol.int/INTERPOL-expertise/Forensics/Facial-recognition.

Introna, Lucas, and Helen Nissenbaum. *Facial Recognition Technology: A Survey of Policy and Implementation Issues*. New York: Center for Catastrophe Preparedness and Response, 2010. https://www.nyu.edu/projects/nissenbaum/papers/facial_recognition_report.pdf.

Ito, Koichi, and Takafumi Aoki. “Recent Advances in Biometric Recognition.” *ITE Transactions on Media Technology and Applications* 6, no. 1 (2018): 64–80. https://doi.org/10.3169/mta.6.64.

ITV News. “Facial Recognition Technology ‘Could Prevent Future Terror Attacks.’” March 1, 2018. http://www.itv.com/news/london/2018-03-01/facial-recognition-technology-could-prevent-future-terror-attacks/.

Jain, Anil K. “Next Generation Biometrics.” Presentation, Michigan State University, December 10, 2009. http://biometrics.cse.msu.edu/Presentations/Next_generation_biometrics_Korea_Dec2010.pdf.

Jain, Surbhi. “Big Data: What, Why and Why Not.” *International Journal of Engineering Development* 5, no. 2 (2017). https://www.ijedr.org/papers/IJEDR1702334.pdf.

Jeberson, W., and Lucky Sharma. “Survey on Big Data for Counter Terrorism.” *International Journal of Innovations and Advancement in Computer Science* 4 (May 2015): 197–205.

Jenkins, Brian M. “Fifteen Years on, Where Are We in the ‘War on Terror?’” Combating Terrorism Center. September 7, 2016. https://ctc.usma.edu/fifteen-years-on-where-are-we-in-the-war-on-terror/.

Kapp, Trevor. “Neighborhood Policing Changing Attitudes and Reaping Benefits, NYPD Says.” DNA Info. April 6, 2017. https://www.dnainfo.com/new-york/20170406/central-harlem/nypd-neighborhood-policing-nco-community-police-department.

Kilgannon, Corey, and Joseph Goldstein. “Sayfullo Saipov, the Suspect in the New York Terror Attack, and His Past.” *New York Times*, November 1, 2017. https://www.nytimes.com/2017/10/31/nyregion/sayfullo-saipov-manhattan-truck-attack.html.

King, Rawlson O’Neil. *Special Report: Biometrics in Law Enforcement*. Lansing, MI: Biometrics Research Group, Michigan State University, 2017. https://www.biometricupdate.com/wp-content/uploads/2017/08/special-report-biometrics-in-law-enforcement.pdf.

Koen, Marthinus C., James J. Willis, and Stephen D. Mastrofski. “The Effects of Body-Worn Cameras on Police Organisation and Practice: A Theory-Based Analysis.” *Policing and Society* (April 2018): 1–17. https://www.tandfonline.com/doi/pdf/10.1080/10439463.2018.1467907?needAccess=true.

Kolkey, Jeff. “How One Illinois City Uses Automatic License Plate Readers and Other Police Tech.” Government Technology. May 21, 2018. http://www.govtech.com/dc/How-One-Illinois-City-Uses-Automatic-License-Plate-Readers-and-Other-Police-Tech.html.

Koper, Christopher S., Bruce G. Taylor, and Daniel J. Woods. “A Randomized Test of Initial and Residual Deterrence from Directed Patrols and Use of License Plate Readers at Crime Hot Spots.” *Journal of Experimental Criminology* 9, no. 2 (June 2013): 213–244. https://www.voiceofsandiego.org/wp-content/uploads/2018/04/Koper-et-al-2.pdf.

Klarreich, Erica. “Hello, My Name Is.” *Communications of the ACM* 57, no. 8 (August 2014): 17–19. https://doi.org/10.1145/2632040.

Kravets, David. “Enhanced DMV Facial Recognition Technology Helps NY Nab 100 ID Thieves.” *Ars Technica*, August 28, 2016. https://arstechnica.com/tech-policy/2016/08/enhanced-dmv-facial-recognition-technology-helps-ny-nab-100-id-thieves/.

Landler, Mark. “Obama Offers New Standards on Police Gear in Wake of Ferguson Protests.” *New York Times*, December 1, 2014. https://www.nytimes.com/2014/12/02/us/politics/obama-to-toughen-standards-on-police-use-of-military-gear.html.

Lane, Julia, Victoria Stodden, Stefan Bender, and Helen Nissenbaum. *Privacy, Big Data, and the Public Good: Frameworks for Engagement*. Cambridge: Cambridge University Press, 2014. https://www.nyu.edu/projects/nissenbaum/papers/BigDatasEndRun.pdf.

Laperruque, Jake. “Preserving the Right to Obscurity in the Age of Facial Recognition.” Century Foundation. October 20, 2017. https://tcf.org/content/report/preserving-right-obscurity-age-facial-recognition/.

Lochner, Sabrina A. “Saving Face: Regulating Law Enforcement’s Use of Mobile Facial Recognition Technology & Iris Scans.” *Arizona Law Review* 55 (2013): 202–233. http://www.arizonalawreview.org/pdf/55-1/55arizlrev201.pdf.

Lum, Cynthia, Julie Hibdon, Breanne Cave, Christopher S. Koper, and Linda Merola. “License Plate Reader (LPR) Police Patrols in Crime Hot Spots: An Experimental Evaluation in Two Adjacent Jurisdictions.” *Journal of Experimental Criminology* 7, no. 4 (2011): 321–345. https://www.voiceofsandiego.org/wp-content/uploads/2018/04/Lum-et-al-2.pdf.

Lynch, Jennifer. *Face Off, Law Enforcement Use of Face Recognition Technology*. San Francisco: Electronic Frontier Foundation, February 12, 2018. https://www.eff.org/wp/law-enforcement-use-face-recognition.

Maass, Dave. “The Four Flavors of Automated License Plate Reader Technology.” Electronic Frontier Foundation. April 6, 2017. https://www.eff.org/deeplinks/2017/04/four-flavors-automated-license-plate-reader-technology.

Maleske, Melissa. “Facial Recognition Presents Privacy Concerns.” Inside Counsel. March 2012. https://www.law.com/almID/4f46a3f8150ba0c00a000048/.

MAS Context. “Ring of Steel.” June 25, 2014. http://www.mascontext.com/issues/22-surveillance-summer-14/ring-of-steel/.

McClain, Noah. “The Horizons of Technological Control: Automated Surveillance in the New York Subway.” *Information, Communication & Society* 21, no. 1 (2018): 46–62. https://doi.org/10.1080/1369118X.2016.1260624.

McCoy, Susan. “O’ Big Brother Where Art Thou?: The Constitutional Use of Facial-Recognition Technology.” *John Marshall Journal of Computer & Information Law* 20, no. 3 (Spring 2002): 471–494.

Mell, Peter, and Timothy Grance. *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*. Special Publication 800–145. Gaithersburg, MD: NIST, September 2011. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Melodia, Mark, Paul Bond, and Angela-Angelovska-Wilson. “Legal Risks and Rules of the Move to Biometrics.” *New York Law Journal*, March 2, 2015. https://www.technologylawdispatch.com/wp-content/uploads/sites/26/2016/02/Legal-NYLJ-Article-Risks-and-Rules-of-the-Move-to-Biometrics.pdf.

Merola, Linda M., and Cynthia Lum. “Understanding Citizen Support for License Plate Readers.” *Translational Criminology* (2015): 1–29. https://www.bja.gov/bwc/pdfs/TC8-Spring2015.pdf#page=25.

Metropolitan Transportation Authority. “Introduction to Subway Ridership.” Accessed September 4, 2017. http://web.mta.info/nyct/facts/ridership/.

Metz, Cade, and Natasha Singer. “Newspaper Shooting Shows Widening Use of Facial Recognition by Authorities.” *New York Times*, July 1, 2018. https://www.nytimes.com/2018/06/29/business/newspaper-shooting-facial-recognition.html.

Miller, Lindsay, and Jessica Toliver. *Implementing a Body-Worn Camera Program: Recommendations and Lessons Learned*. Washington, DC: Community Oriented Policing Services, 2014. https://www.justice.gov/iso/opa/resources/47201491213471524686 9.pdf.

Möllers, Norma, and Jens Hälterlein. “Privacy Issues in Public Discourse: The Case of ‘Smart’ CCTV in Germany.” *Innovation: European Journal of Social Sciences* 26 (March 1, 2013): 65–87. https://publishup.uni-potsdam.de/opus4-ubp/frontdoor/deliver/index/docId/7767/file/moellers_diss.pdf#page=73.

Moriarty, Laura J., ed. *Criminal Justice Technology in the 21st Century*. 3rd ed. Springfield, IL: Charles C. Thomas Publisher, 2017.

Moy, Laura M., Harrison Rudolph, and Alvaro M. Bedoya. *Not Ready for Takeoff: Face Scans at Airport Departure Gates*. Washington, DC: Center on Privacy and Technology, Georgetown Law, December 21, 2017. https://www.airportfacescans.com/sites/default/files/Biometrics_Report__Not_Ready_For_Takeoff.pdf

Moynihan, Colin. “Driver Charged with Manslaughter in Deaths of 2 Children.” *New York Times*, May 3, 2018. https://www.nytimes.com/2018/05/03/nyregion/driver-manslaughter-brooklyn-children.html.

Mozur, Paul. “Inside China’s Dystopian Dreams: A.I., Shame and Lots of Cameras.” *New York Times*, July 9, 2018. https://www.nytimes.com/2018/07/08/business/china-edsurveillance-technology.html.

Ms. Smith [pseud.]. “You Consent to a Search If a Camera Sees You?: Facial Recognition vs. 4th Amendment.” CSO. March 22, 2012. https://www.csoonline.com/article/2221971/microsoft-subnet/you-consent-to-a-search-if-a-camera-sees-you--facial-recognition-vs-4th-amendment.html.

Mullins, J. “Ring of Steel II: New York City Gets Set to Replicate London’s High-Security Zone.” *IEEE Spectrum* 43, no. 7 (July 2006): 12–13. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1652996.

Munger, Kristen, and Shelby J. Harris. “Effects of an Observer on Handwashing in a Public Restroom.” *Perceptual and Motor Skills* 69 (1989): 733–734. https://kmunger.files.wordpress.com/2007/09/munger-harris-1989-effects-of-an-observer-on-handwashing-in-a-public-restroom.pdf.

National Alliance on Mental Illness. “Mental Health by the Numbers.” Accessed June 17, 2018. https://www.nami.org/Learn-More/Mental-Health-By-the-Numbers.

National Conference of State Legislatures. “Automated License Plate Readers: State Legislation 2016 & 2017.” Accessed May 6, 2018. http://www.ncsl.org/research/telecommunications-and-information-technology/automated-license-plate-readers-state-legislation-2016.aspx.

National Law Enforcement Officers Memorial Fund. *2017 End of Year Officer Fatalities Report*. Washington, DC: NLEOMF, 2017. http://www.nleomf.org/assets/pdfs/reports/fatality-reports/2017/2017-End-of-Year-Officer-Fatalities-Report_FINAL.pdf.

National Telecommunications and Information Administration. “Privacy Best Practice Recommendations for Commercial Facial Recognition Use.” Accessed March 28, 2018. https://www.ntia.doc.gov/files/ntia/publications/privacy_best_practices_recommendations_for_commercial_use_of_facial_recogntion.pdf.

NEC Global Face Recognition Centre of Excellence. *NeoFace Watch, High Performance Face Recognition*. NEC Global Face Recognition Centre of Excellence, 2016. https://www.nec.com/en/global/solutions/safety/face_recognition/PDF/Face_Recognition_NeoFace_Watch_Brochure.pdf.

———. “Technology.” Accessed April 15, 2018, http://www.nec.com/en/global/solutions/safety/Technology/FaceRecognition/index.html.

Newell, Bryce Clayton. “Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy, and Access to Government Information.” *Maine Law Review* 66 (2013): 1–42.

New York City Police Department. “Build the Block.” Accessed July 17, 2018. https://www1.nyc.gov/site/nypd/bureaus/patrol/buildtheblock.page.

———. “Counterterrorism.” Accessed May 14, 2018. https://www1.nyc.gov/site/nypd/bureaus/investigative/counterterrorism.page.

———. “Crime Statistics.” Accessed July 17, 2018. https://www1.nyc.gov/site/nypd/stats/crime-statistics/crime-statistics-landing.page.

———. “Midtown Manhattan Security Initiative.” Press release, NYPD, September 20, 2010. http://www.nyc.gov/html/nypd/html/pr/pr_2010_midtown_security_initiative.shtml.

———. *Patrol Guide: Command Operations*. 212–123. New York: NYPD, January 8, 2018. https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/body-worn-cameras-patrol-guide.pdf.

———. *Patrol Guide: “Padlock Law” Program*. 291–31. New York: NYPD, July 1, 2014. https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/public-pguide3.pdf.

New York State Division of Criminal Justice Services. *Operation of License Plate Readers in New York State: Suggested Guidelines*. Albany: NYS DCJS, June 2017. https://www.aclu.org/files/FilesPDFs/ALPR/new-york/alprpra_rensselaercountysheriffdepartment_troyny_2.pdf.

New York State Governor’s Office. “Governor Cuomo Announces More Than 100 Arrests since Major Enhancement to DMV’s Facial Recognition Technology.” August 24, 2016. https://www.governor.ny.gov/news/governor-cuomo-announces-more-100-arrests-major-enhancement-dmvs-facial-recognition-technology.

New York State Senate. “Senate Bill S23.” Last modified December 28, 2016. https://www.nysenate.gov/legislation/bills/2017/S23.

Nissenbaum, Helen Fay. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Palo Alto, CA: Stanford University Press, 2010.

Nolan, Lucas. “Facebook Could Face Billions in Fines over Facial Recognition Features.” Breitbart. April 17, 2018. http://www.breitbart.com/tech/2018/04/17/facebook-could-face-billions-in-fines-over-facial-recognition-features/.

NYPD News. “Finest Technology Helps New York’s Finest Take Two Guns off the Streets.” December 8, 2015. http://nypdnews.com/2015/12/finest-technology-helps-new-yorks-finest-take-two-gun-off-the-streets/.

O'Reilly, Kathleen. "Transparency, Accountability, and Engagement: A Recipe for Building Trust in Policing." Master's thesis, Naval Postgraduate School, June 2017.

Orr, Steve. "New York Knows Where Your License Plate Goes." *USA Today*, July 28, 2014. https://www.usatoday.com/story/news/nation-now/2014/07/28/new-york-archiving-license-surveillance-data/13261679/.

People's Daily Online. "'Skynet' System Supported by Facial Recognition Technology Boosts Chinese Public Safety." March 26, 2018. http://en.people.cn/n3/2018/0326/c90000-9441798.html.

Perez, Bien. "Shanghai Subway to Use Alibaba Voice and Facial Recognition Technologies." *South China Morning Post*, December 5, 2017. http://www.scmp.com/tech/enterprises/article/2123014/shanghai-subway-use-alibaba-voice-and-facial-recognition-systems-ai.

Peterson, Andrew H., Jesse L. Kirkpatrick, and Deborah A. Boehm-Davis. *Developing Ethical, Legal, and Policy Analyses Relevant to the Use of Machine Learning Algorithms in National Security*. White paper, George Mason University, 2017. http://sites.nationalacademies.org/cs/groups/dbassesite/documents/webpage/dbasse_179882.pdf.

Phantom Plate. "Avoid Red Light and Speed Camera Tickets." Accessed April 20, 2018. https://www.phantomplate.com/.

Phillips, P. Jonathan, Patrick J. Flynn, Keven W. Bowyer, Richard W. Vorder Bruegge, Patrick J. Grother, George W. Quinn, and Matthew Pruitt. "Distinguishing Identical Twins by Face Recognition." In *Face and Gesture*, 185–192. Piscataway, NJ: IEEE, 2011. https://doi.org/10.1109/FG.2011.5771395.

Photo Blocker. "Avoid Red Light and Speed Camera Tickets." Accessed April 21, 2018. https://www.photoblocker.com/photoblocker.html.

Quintin, Cooper, and Dave Maass. "License Plate Readers Exposed! How Public Safety Agencies Responded to Major Vulnerabilities in Vehicle Surveillance Tech." Electronic Frontier Foundation. October 28, 2015. https://www.eff.org/deeplinks/2015/10/license-plate-readers-exposed-how-public-safety-agencies-responded-massive.

Ramachandra, Raghavendra, and Christoph Busch. "Presentation Attack Detection Methods for Face Recognition Systems: A Comprehensive Survey." *ACM Computing Surveys* 50, no. 1 (March 20, 2017): 1–37. https://doi.org/10.1145/3038924.

Riffat, Muzamil. “Legal Aspects of Privacy and Security: A Case- Study of Apple versus FBI Arguments.” Sans Institute. June 1, 2016. https://www.semanticscholar.org/paper/Legal-Aspects-of-Privacy-and-Security%3A-A-Case-Study/5f9139b8aa661bd040eec464d16ce31fbb829af5.

Risen, Tom. “Could the FBI See Your Selfies?” *U.S. News & World Report*, July 8, 2014. https://www.usnews.com/news/articles/2014/07/08/fbi-may-seek-facebook-data-for-facial-recognition.

Robbins, Liz. “Activists and ICE Face Off over Detained Immigrant Leader.” *New York Times*, January 12, 2018. https://www.nytimes.com/2018/01/12/nyregion/immigration-activist-deportation.html.

Roberts, David J., and Meghann Casanova. *Automated License Plate Recognition Use by Law Enforcement: Policy and Operational Guide, Summary*. Doc. 239605. Alexandria, VA: International Association of Chiefs of Police, September 2012. https://www.ncjrs.gov/pdffiles1/nij/grants/239605.pdf.

San Diego County Sheriff’s Department. “Home Page.” Accessed May 29, 2018. http://www.sdsheriff.net/tmh/docs/tmh-english.pdf

Sandoval, Greg. “Over 100 Amazon Employees, Including Senior Software Engineers, Signed a Letter Asking Jeff Bezos to Stop Selling Facial-Recognition Software to Police.” *Business Insider*, June 22, 2018. http://www.businessinsider.com/over-100-amazon-employees-sign-letter-jeff-bezos-stop-selling-facial-recognition-software-police-2018-6.

Savransky, Rebecca. “De Blasio: NYPD Planning to Have Body Camera on Every Cop by Year’s End.” *The Hill*, January 31, 2018. http://thehill.com/homenews/state-watch/371582-de-blasio-says-nyc-planning-to-have-every-cop-equipped-with-body-camera.

Seaskate. *The Evolution and Development of Police Technology*. Washington, DC: Seaskate, July 1, 1998. https://www.ncjrs.gov/pdffiles1/Digitization/173179NCJRS.pdf.

Shay, Jim. “License Plate Reader Help Nab Suspect in Slaying of NYPD Explorer.” Officer. July 11, 2018. https://www.officer.com/command-hq/technology/traffic/lpr-license-plate-recognition/news/21012850/license-plate-reader-help-nab-suspect-in-slaying-of-nypd-explorer-lesandro-junior-guzmanfeliz.

Siff, Andrew. “New MTA Towers Can Read License Plates, and Maybe More.” NBC (New York). September 28, 2017. http://www.nbcnewyork.com/news/local/MTA-Bridge-and-Tunnel-Gateway-Towers-Can-Read-License-Plates-Security--448568193.html.

Silverman, Eli B. *NYPD Battles Crime: Innovative Strategies in Policing*. Boston: Northeastern University Press, 1999.

Skirpan, Michael, and Tom Yeh. "Designing a Moral Compass for the Future of Computer Vision Using Speculative Analysis." In *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 64–73. Piscataway, NJ: IEEE, 2017. http://openaccess.thecvf.com/content_cvpr_2017_workshops/w16/papers/Yeh_Designing_a_Moral_CVPR_2017_paper.pdf.

Stanley, Jay. *Police Body-Mounted Cameras: With Right Policies in Place, a Win for All*. Version 2.0. New York: American Civil Liberties Union, March 2015. https://www.aclu.org/other/police-body-mounted-cameras-right-policies-place-win-all.

Statista. "Number of Motor Vehicles Registered in the United States from 1990 to 2016 (in 1,000s)." Accessed June 3, 2018. https://www.statista.com/statistics/183505/number-of-vehicles-in-the-united-states-since-1990/.

Sunflex Zone. "SunflexZone Anti-ALPR & Red-Light Camera Privacy Solutions." Accessed June 9, 2018. https://www.sunflexzone.com/.

Sydell, Laura. "It Ain't Me, Babe: Researchers Find Flaws in Police Facial Recognition Technology." NPR. October 25, 2016. http://www.npr.org/sections/alltechconsidered/2016/10/25/499176469/it-aint-me-babe-researchers-find-flaws-in-police-facial-recognition.

Tempey, Nathan. "The NYPD Is Tracking Drivers across the Country Using License Plate Readers." Gothamist. January 26, 2016. http://gothamist.com/2016/01/26/license_plate_readers_nypd.php.

Townsend, Mark. "Police to Use Facial-Recognition Cameras at Cenotaph Service." *Guardian*, November 11, 2017. http://www.theguardian.com/technology/2017/nov/12/metropolitan-police-to-use-facial-recognition-technology-remembrance-sunday-cenotaph.

UK Parliament. "Protection of Freedoms Bill." Accessed August 8, 2008. https://publications.parliament.uk/pa/cm201011/cmpublic/protection/memo/pf11.htm.

U.S. Congress. House of Representatives. *Hearing before the Committee to Review Law Enforcement's Policies on Facial Recognition Technology*. 115th Cong., 1st sess., March 22, 2017. https://oversight.house.gov/hearing/law-enforcements-use-facial-recognition-technology.

U.S. Immigration and Customs Enforcement. *Acquisition and Use of License Plate Reader Data from a Commercial Service*. DHS-ICE-PIA-039. Washington, DC: Department of Homeland Security, December 2017. https://www.dhs.gov/publication/dhs-ice-pia-039-acquisition-and-use-license-plate-reader-data-commercial-service.

Vocativ. "Memo: New York Called for Face Recognition Cameras at Bridges, Tunnels." Last modified January 27, 2017. http://www.vocativ.com/396745/memo-new-york-called-for-face-recognition-cameras-at-bridges-tunnels/.

Voelz, Glenn J. *Rise of iWar: Identity, Information, and the Individualization of Modern Warfare*. New York: Skyhorse Publishing, 2018. https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1292.

Waddell, Kaveh. "How License-Plate Readers Have Helped Police and Lenders Target the Poor." *Atlantic*, April 22, 2016. https://www.theatlantic.com/technology/archive/2016/04/how-license-plate-readers-have-helped-police-and-lenders-target-the-poor/479436/.

Waitt, Tammy. "CUBIC Testing Face Recognition for Subway (Learn More, Video)." American Security Today. October 10, 2017. https://americansecuritytoday.com/cubic-testing-face-recognition-subway-learn-video/.

Wexler, Chuck. "Introduction." In *How are Innovations in Technology Transforming Policing*, i–ii. Washington, DC: Police Executive Research Forum, January 2012. http://www.policeforum.org/assets/docs/Critical_Issues_Series/how%20are%20innovations%20in%20technology%20transforming%20policing%202012.pdf.

White, Michael D., and Henry F. Fradella. *Stop and Frisk: The Use and Abuse of a Controversial Policing Tactic*. New York University Press, 2016.

Wood, Matt. "Some Quick Thoughts on the Public Discussion Regarding Facial Recognition and Amazon Rekognition This Past Week." *AWS New Blog*, June 1, 2018. https://aws.amazon.com/blogs/aws/some-quick-thoughts-on-the-public-discussion-regarding-facial-recognition-and-amazon-rekognition-this-past-week/.

Woodward, John D., Jr., Christopher Horn, Julius Gatune, and Aryn Thomas. *Biometrics: A Look at Facial Recognition*. Santa Monica, CA: RAND Corporation, 2003. http://www.dtic.mil/dtic/tr/fulltext/u2/a414520.pdf.

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