

Spring 6-11-2022

A Comparative Analysis of Best Practices in a Facial Recognition Policy for Law Enforcement Agencies

Terry H. Smith
DePaul University

Follow this and additional works at: https://via.library.depaul.edu/soe_etd



Part of the [Educational Leadership Commons](#)

Recommended Citation

Smith, Terry H., "A Comparative Analysis of Best Practices in a Facial Recognition Policy for Law Enforcement Agencies" (2022). *College of Education Theses and Dissertations*. 236.
https://via.library.depaul.edu/soe_etd/236

This Capstone is brought to you for free and open access by the College of Education at Via Sapientiae. It has been accepted for inclusion in College of Education Theses and Dissertations by an authorized administrator of Via Sapientiae. For more information, please contact digitalservices@depaul.edu.

A Comparative Analysis of Best Practices in a Facial Recognition Policy for Law Enforcement Agencies

A Capstone in Education with a Concentration in Educational Leadership

By: Terry Smith

DePaul University

College of Education

© 2022 Terry Smith

Submitted in Partial Fulfillment of the Requirements for the
Degree of Doctor of Education

June 2022

Facial Recognition Policy

I approve of the Capstone of Terry Smith



Andrea Kayne

Program Director &

Associate Professor in Educational Leadership

DePaul University

Capstone Advisor

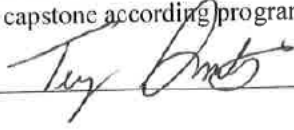


Date

Certification of Authorship

I certify that I am the sole author of this capstone. Any assistance received in the preparation of this capstone has been acknowledged and disclosed within it. Any sources utilized, including the use of data, ideas and words, those quoted directly or paraphrased, have been cited. I certify that I have prepared this capstone according program guidelines as directed.

Author Signature



Date 05-07-22

Executive Summary

Facial Recognition Technology (FRT) and the plethora of applications that have adopted this technology have exploded in the last decade. Most people have probably heard about local law enforcement agencies utilizing FRT to catch criminals, locate missing persons, and provide large-scale event security. However, others may not realize FRT has the ability to unlock their phones, tag their friends in social media accounts, and allow users access into restricted spaces such as their own homes.

In 2011, it was reported that over one-half of adult Americans have their image stored in facial recognition databases that are accessible by law enforcement officials. The American Civil Liberties Union (ACLU) states that the Federal Bureau of Investigations (FBI) has obtained over 640 million photographs in the agency's database.

Law enforcement's use of FRT has been criticized since its implementation. Critics have lambasted FRT, citing inaccuracy of the technology; potential race, age, and gender bias; the collection and retention of images; and a lack of governing standards as to when the technology can be applied. In addition, the lack of transparency has been met with fierce pushback as entities such as the ACLU have filed multiple lawsuits against federal agencies in an attempt to garner additional information on the use and practices of FRT within these agencies.

This research paper will discuss multiple aspects of Facial Recognition Technology. A brief history of the technology will be given along with an overview of how FRT works and its implementation in law enforcement agencies, as well as in private sector settings. This paper will also review new and existing laws at the state, local, and federal level. Issues over the misuse of FRT, concerns of civil rights activists, and limitations of FRT will be conveyed. Police department policies governing the use of FRT will also be explored in detail.

This study examines FRT policies from seven law enforcement agencies across the country. Specific elements have been identified by the author as essential components required to possess an effective FRT policy. These policies will be compared and discussed, highlighting the inclusion or absence of these essential elements. In addition, a comprehensive comparative law review was conducted with a focus on the Confrontation Clause, rules of admissibility and the Fourth Amendment concerning criminal proceedings involving fingerprint and DNA evidence. This review will be used as the basis for a predictive model of the future pathway that awaits FRT upon its introduction into criminal trials.

Additionally, this paper will give recommendations for a law enforcement agency to create a FRT policy utilizing current best practices that will allow this technology to be introduced and accepted into evidence in future criminal proceedings. Finally, the findings will be discussed, implications will be examined, and suggestions for further research and the importance of such, will be offered.

Table of Contents

List of Tables	viii
List of Figures	ix
Introduction.....	1
Problem Statement	1
Purpose Statement.....	1
Research Questions	2
Overview of the Methodology	2
Rationale and Significance	2
Role of the Researcher	3
Researcher Assumptions	3
Definition of Key Terms	3
Literature Review.....	5
History of Facial Recognition	5
FERET.	5
Current technologies	5
How Facial Recognition Works.....	6
Face detection	7
Face analysis	7
Converting the image to data	7
Finding a match.....	7
Governmental Utilization.....	8
Local Law Enforcement Applications	8
Camera usage	8
Body worn cameras.....	9
Reasons for and against	9
Federal Law Enforcement Applications	9
Next Generation Identification system	9
Applications by federal agencies	10
Current Law	11
Federal statutes.....	11
State legislation.....	12
Local ordinances	13
Current Legal Challenges	14

Lynch v. State	15
People v. Reyes	15
Confrontation Clause	16
Issues with Confrontation Clause	16
Hearsay rule	17
Issues with Hearsay rule	17
Fourth Amendment	17
Methodology	19
Conceptual Framework	19
Rationale for Research Tradition	19
Literature Search Strategies	20
Data Collection	20
Document Review	20
Data Analysis Methods	21
Comparative law review	21
Policy evaluation	22
Overview of the Sample	27
Issues of Trustworthiness	27
Limitations	28
Results	29
Comparative Law Review	29
Fingerprint historical account	29
DNA historical account	30
Rules of Admissibility	32
Summary of the case	32
Similarities/differences	33
Evaluation	33
Confrontation Clause / Hearsay Rule	34
Summary of the case	34
Similarities/differences	35
Evaluation	36
Fourth Amendment	36
Summary of the case	36
Similarities/differences	38

Evaluation 38

Review of Policies 39

Discussion 46

Law Review 46

 Laws and regulations 46

 Legal challenges..... 46

Policy Discussion..... 49

Recommendations..... 56

 Recommendation 1: Invoke Stakeholder Involvement..... 56

 Recommendation 2: Create a Working Group..... 57

 Recommendation 3: Create a Training Program 58

 Recommendation 4: Finalize and Implement Policy 58

Conclusion 60

 Implications..... 60

 Suggestions for Future Research 60

References..... 61

Appendix A: Sample Policy..... 70

List of Tables

Table 1. States Using Frye Rule	323
Table 2. Similarities of Fingerprint and DNA in Admissibility Rulings	33
Table 3. Differences of Fingerprint and DNA in Admissibility Rulings.....	33
Table 4. Similarities of Fingerprint and DNA Confrontation Clause / Hearsay Rulings	36
Table 5. Differences of Fingerprint and DNA Confrontation Clause / Hearsay Rulings	37
Table 6. Similarities of Fingerprint and DNA in Fourth Amendment Rulings	39
Table 7. Largest Police Departments in the U.S.....	40
Table 8. Police Polices	40
Table 9. Evaluation of Police Department Polices	42
Table 10. Describes the Process of FRT	43
Table 11. Specifies the Restrictions of the Utilization of FRT.....	43
Table 12. Specifies the Oversight Process of FRT	44
Table 13. Specifies the Verification Mechanisms of FRT	45
Table 14. Details the Record Keeping Practices.....	45

List of Figures

Figure 1. FRT Process.....	7
Figure 2. Example of Policy Evaluation Template.....	25

Introduction

Problem Statement

Facial recognition technology is a recent phenomenon that has become a controversial issue when employed by law enforcement agencies. Civil rights activists have denounced this technology as intrusive and a violation of the public's Fourth Amendment rights. However, members of law enforcement have embraced this technology as a tool that allows them to identify bad actors at large-scale events, missing or wanted persons, and identification of suspected criminals. An increasingly contentious issue is that some law enforcement agencies contract this technology through third-party vendors, such as Amazon Rekognition, a cloud-based software developed by Amazon and sold to government agencies (Amazon, n.d).

The ability of law enforcement agencies to implement FRT programs has changed drastically in the last few years as local, state, and federal laws and regulations have been implemented, along with the reluctance of third-party vendors to work with governmental agencies. As a result, several municipalities have disallowed law enforcement agencies from acquiring FRT programs, while others have categorically denied law enforcement the ability to utilize the technology outside of a stringent process containing specific sets of circumstances.

Furthermore, FRT has yet to meet the rigorous requirements that will allow for the technology to become admissible in criminal court proceedings. The Confrontation Clause, Hearsay Rule, and the Fourth Amendment are hurdles that may require years of legal rulings and challenges that will inevitably delay the introduction of this technology into a court of law. Nevertheless, as FRT programs become more accurate, the likelihood that this technology will play a significant role in the investigation and apprehension of suspect criminals will rise exponentially.

Purpose Statement

This non-experimental, collective case study research project aims to introduce the basic foundations of FRT programs and define some commonly used terminology in the industry. In addition, an overview of various law enforcement FRT programs will be presented.

This paper will also review new and existing laws at the state, local, and federal levels. Issues over the misuse of FRT, concerns of civil rights activists, and limitations of FRT will be conveyed. Police department policies governing the use of FRT will also be explored in detail.

Through the completion of this project, a law enforcement agency shall be able to create a FRT policy that will follow industry best practices, comply with recent law and regulations, offer solutions for the implementation of this technology to survive the upcoming legal rigors that await, and offer a fair and equitable set of guidelines that will offer constitutional protections to the general public.

Research Questions

What are the best practices for creating a Facial Recognition Policy to be implemented by a law enforcement agency that will comply with existing laws and ordinances while offering the greatest protection to Americans' civil rights? What steps should an agency include in this policy to ensure this technology will stand up to the rigor of legal challenges as FRT is introduced into the criminal court system as evidence?

Overview of the Methodology

This study will be a non-experimental collective case study design informed by constructivist data analysis methods. This approach has been utilized in other studies to examine technology applications used by law enforcement agencies, such as: technology in law enforcement (Thorkildsen et al., 2019), a case study on the impact of mobile broadband data access to law enforcement (Carter & Grommon, 2014), and predictive policing (Perry et al., 2013). Using this approach in this study allowed for the data to be scrutinized and conceptualized without rendering the data objective (Charmaz, 2008).

Constructivist data analysis methods aim to collect and analyze data through inductive means to develop theoretical analyses (Charmaz, 2013). This framework is prudent in this particular instance as "data does not provide a window on reality. Rather, the 'discovered' reality arises from the interactive process, and its temporal, cultural, and structural contexts" (Charmaz, 2000). In the context of this research, the data will reflect information gleaned from previous court rulings, statistics regarding FRT, and police department policies.

Rationale and Significance

The importance of creating a fair and equitable FRT policy for law enforcement agencies is intensifying as lawmakers rush to pass legislation restricting and even banning this technology altogether. California, Oregon, Washington, and New Hampshire are a few states that have already passed legislation regulating the use of FRT by police agencies (Greenberg, 2020). In addition, municipalities such as Boston, Portland, and San Francisco have passed laws prohibiting local officials from using FRT software in public areas (Keene, 2020).

When used correctly, this technology has the capability of becoming an invaluable tool for law enforcement. Conversely, if this technology were misused, the constitutional rights of United States citizens would be violated. I believe that if more people were aware of the capabilities and limitations and knew that there is a standardized policy and set of procedures to regulate the circumstances in which this technology may be applied, more people would accept its implementation and utilization.

Role of the Researcher

As the researcher conducting this study, it is important to disclose that I am currently and have been employed for the last sixteen years as a Chicago Police Officer. Over the last four years I have been assigned in an investigative role as a violent crimes / homicide detective. I bring an understanding to the research question as a law enforcement officer and acknowledge the benefits that this technology is capable of producing. As a civilian, I strongly advocate for the right to privacy and protections afforded to me under the Fourth Amendment, and I champion policies that will prevent governmental agencies from misusing or overstepping said protections.

Researcher Assumptions

It is my assumption that a majority of law enforcement agencies have not created a FRT policy. One reason may be due to the limited application of this technology. A second reason may be that some agencies would prefer not to document the methods in which FRT is employed, lest they be subject to Freedom of Information Act requests. This is my assumption and would be nearly impossible to prove, but lacking a standardized policy and procedure greatly diminishes the ability for an outside source to gain hold of the most accurate information regarding FRT usage.

Definition of Key Terms

Biometrics - body measurements and characteristics unique to an individual person that are utilized for automated recognition: e.g., fingerprints, palm prints, and iris scans (DHS(b), 2020).

Face Recognition Algorithm - consists of two parts (1) face detection and normalization and (2) face identification (Phillips et al., 1999).

Facial Recognition Technology - computer systems that analyze images of human faces for the purposes of identifying them (ACLU, 2020).

Faceprint - digital scan / photograph of a face that identifies an individual based on unique characteristics of the facial structure that is as unique to a specific person as a fingerprint (Faceprint, 2020).

False Positive - occurs when one or multiple suggested matches differ from the input image (AAMVA, 2019).

Nodal points - various peaks and valleys that make up facial features, also referred to as landmarks. The human face consists of approximately 80 nodal points (Bonsor & Johnson, 2001).

Policy - a course of action adopted by an agency that provides guidance on a particular issue (Merriam-Webster, n.d.).

Probability / Match Score - score given to the probability that one image matches another (AAMVA, 2019).

Probe photo - photograph of an individual that law enforcement officials are seeking to identify (CRS, 2020). Also referred to as "input image."

Standardized - "to bring into conformity with a standard, especially in order to assure consistency and regularity" (Merriam-Webster, n.d.).

Similarity score - score assigned based on the probability that the returned image is a match for the target image

Target photos - photographs that are returned based on the parameters of the threshold, or similarity score to the probe photo or input image (CRS, 2020). Also referred to as "comparison photo" and "returned photo."

Literature Review

History of Facial Recognition

In the early 1960's, Woodrow Bledsoe created the first program designed for facial recognition (Raviv, 2020). Through his company, Panoramic Research Incorporated, Bledsoe was the recipient of funding provided by the Central Intelligence Agency (CIA) for numerous projects involving automated reasoning and artificial intelligence (Brice, 2020). As many of Bledsoe's projects were funded by the secretive government agency, much of his research has gone unpublished (Norman, n.d.).

Bledsoe coined a technique named man-machine facial recognition. This technique involved a human manually entering a set of grid points from a photograph into a RAND tablet, a graphical computer input device (Nilsson, 2009). The RAND tablet would then locate and assign coordinate locations to specified facial features (Lydick, n.d.). The coordinate locations of a subject's hairline, eyes, and nose, among others, would then be recorded and measured, and the numerical data would be inserted into a database (Lydick, n.d.). Upon entry into the database the program would then find and select the image most closely resembling the provided sample (Gates, 2004).

While Bledsoe's work was revolutionary, it was bound by the available technology of his era. Bledsoe himself noted many of the limitations of this new technology. Photographs of the same individual could confuse computer algorithms based on varying angles, environments, poses, lighting conditions, and age of the individual when the photo was taken (Lydick, n.d.).

FERET. The next major breakthrough was in 1993, during the creation of the Facial Recognition Technology (FERET) program (Gates, 2011). This program was developed by the Defense Advanced Project Research Agency and the Army Research Lab with an objective of developing a common database of facial imagery that researchers could access to use as a baseline for facial recognition algorithm testing (Phillips et al., 1999).

According to the National Institute of Standards and Technology (NIST) Interagency Report 6264, facial recognition began to develop at a rapid pace during this time period based on three technological developments: new computer algorithms, new methods for evaluating the performance of these computer algorithms, and the availability of larger facial image databases (Phillips et al., 1999). FERET databases standardized the interpretation of results, which allowed for institutions to compare algorithm models among their peers. The marketing of private industry FRT companies began shortly thereafter, with multiple organizations forming that used their results on the FERET tests as selling points (Gates, 2011).

Current technologies. By the late 2000's companies such as Google and Facebook had accumulated hundreds of millions of images, thus overcoming preprocessing limitations that had hindered past research groups (Brice, 2020). No longer would researchers be bound to small sample sizes. Organizations such as the NIST now scrape images from social media sites, Google images, and YouTube videos to increase the size of their datasets (Solon, 2019).

Other technological advancements have allowed for the creation of algorithms that can detect facial features in real-time and object identification in videos (Viola & Jones, 2004). Some

companies employ 3-D face modeling technology. This allows for 3-D models to be created from 2-D photographs, creating a "faceprint" (Lydick, n.d.). Computer software is also capable of entering images or photographs into a program that will then seek out specific objects or individuals in real-time video feeds (BriefCam, 2020).

Another principal advancement for FRT has been the development of deep learning technology or, more specifically, convolutional neural network (CNN). CNNs are typically found in FRT and have led to a drastic reduction in error rates (Ciresan, et al., 2012). CNNs require a large dataset of images so that the computer program can "learn" and become more proficient (Wang & Li, 2018). CNN has become the preferred method in FRT as it can perform "segmentation, feature extraction and classification in one processing module with minimal pre-processing tasks on the input image" (Syafeeza et al., 2014, p. 45).

The addition of advanced algorithms, faster computer processors, and larger datasets has also led to an increase in accuracy. Currently, programs are able to distinguish between identical sets of twins with a 90% success rate (Phillips et al., 2011). In 2018, the NIST Interagency Report 8238 tested 127 algorithms from 39 different vendors (NIST, 2018). Researchers performed a "one to many" test in which a photograph of an individual was entered into a large database containing over 26 million photographs (NIST, 2018). At the conclusion, it was found that these searches were successful 99.8% of the time, up from 96% in 2014 (NIST, 2018). Critics of this report stated that the performance of FRT relies heavily on ideal conditions, and the accuracy of these programs would be greatly diminished in real-world scenarios (Sample, 2019).

How Facial Recognition Works

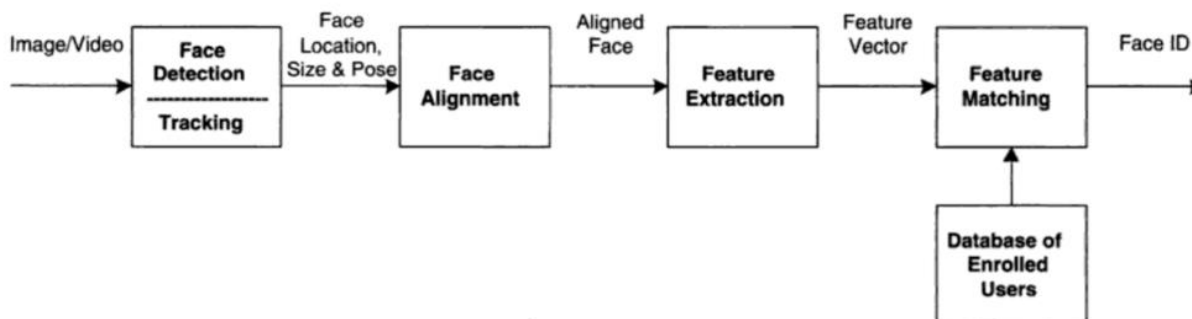
The foundation of FRT can be broken down into four-part process (Dwivedi, 2019):

1. Face detection - a camera will detect and recognize a human face
2. Face analysis - software will analyze the face's nodal points
3. Converting the image to data - each nodal point will be assigned a numerical value which will then be converted to a "faceprint"
4. Finding a match - faceprint is then compared to a database of facial codes and attempts to locate a match.

The following illustration appears courtesy of Li and Jain's (2005) *Handbook of Face Recognition* and depicts the facial recognition process (p. 3).

Figure 1. FRT Process

FRT Process



Face detection. Historically, one of the greatest challenges to face detection has been the achievement of high levels of accuracy when used in uncontrolled conditions (Shepley, n.d.). Facial detection algorithms often will attempt to locate human eyes in a photograph, as they are located in a "valley" and are typically one of the easiest features to detect (Miller, 2019). Upon detection of eyes, the algorithm will attempt to locate and map other facial features such as nose, mouth, and iris (Miller, 2019). Once the computer algorithm is satisfied that a facial region has been detected, it can then begin running additional validation techniques (Miller, 2019). In addition to face detection, algorithms have been created to assist with facial expression recognition, face tracking, tagging of photographs on social media sites, and auto focusing on smartphones (Shepley, n.d.).

Face analysis. In this stage, programs begin mapping out an individual's facial nodal features (Dwivedi, 2019). Calculations between these nodal features, such as the distance between the eyes, are measured and then stored (Klosowski, 2020). Typically, 2-D images are used rather than 3-D, as 2-D images are more likely to be found as comparison images stored in databases (Panda Security, 2020).

Converting the image to data. This step in the process can vary greatly depending on the algorithm being utilized by the program. According to NIST, there are 127 commonly used algorithms currently in use (NIST, 2018). These algorithms can vary based on lighting, head tilt, and other external variables presented by the captured image (Dwivedi, 2019).

The measurements that were taken in the face analysis stage are then assigned a numerical value (Dwivedi, 2019). These values are then coded, and the program creates a faceprint (Panda, 2020). Faceprints are unique to the individual, much like a person's fingerprint (Faceprint, 2020).

Finding a match. According to Amazon Web Services (n.d.), after target images are scored and processed through a database, the results are returned by a similarity score based on the probability that the returned image is a match for the target image. Matches are either utilized for verification or identification. Verification is when the program will match the target photo to a known identity (GAO, 2020). This process is referred to as a one-to-one comparison and can be found on applications such as those that will unlock a user's smartphone. Identification is a one-to-many

search is when the target image is compared to a large number of comparable photographs with the end goal of matching the target to an individual in a dataset (GAO, 2020).

Governmental Utilization

The Department of Motor Vehicles (DMV) is thought to be one of the first government agencies to implement an FRT program. New Mexico and West Virginia introduced their programs shortly after the FERET study, with the goal of preventing persons from obtaining multiple driver's license under different names (Gate, 2011). Currently, DMVs in at least 43 states are equipped with FRT capabilities, and that number is expected to climb, as all 50 states are now in compliance with the requirements of the RealID Act (DHS(a), 2020; Kelley, 2020).

The RealID Act created minimum security standards that states must meet to gain compliance, one of which was installing systems that would reduce the ability for a person to obtain an ID under a fraudulent name (DHS(b), 2020). As of 2018, there were over 227 million driver's licenses issued across the United States (Wagner, 2020). As of September 2020, 105 million of these driver's license and identification cards were RealID compliant (DHS(b), 2020).

One of the loudest criticisms regarding FRT use by DMVs is the access that is given to law enforcement agencies. Currently 27 states allow the FBI to search their database of photographs (Kelley, 2020). These databases have also become a source for officials at the Immigration and Customs Enforcement now that a dozen states allow for undocumented immigrants to obtain driver's license privileges (Harwell, 2019).

Local Law Enforcement Applications

Nearly one in four police departments across the country have access to FRT (Ghaffary, 2019). Police departments can now capture images for comparison from surveillance cameras, red light and speed cameras, and, most recently, body worn cameras. It is believed that in 25% of criminal cases police have access to photographs of the suspect or accomplice during the commission of the crime (Petrov, 2012). These photographs then become available for inclusion into an FRT program consisting of departmental booking photographs. Additionally, departments have the ability to purchase databases from third-party vendors or utilize other governmental databases when comparing images. While the technology has been used in some high-profile cases, more often than not search inquiries are related to "routine" criminal investigations (Ghaffary, 2019).

Camera usage. Surveillance techniques being conducted by local police departments has become increasingly ubiquitous. Major U.S. police departments such as Chicago and New York boast an impressive amount of surveillance cameras linked to their systems. Chicago Police officers have access to over 32,000 cameras, while New York Police Department members can view over 9,000 (Glanton, 2019; Pasley, 2019). These estimates do not include private surveillance cameras that officers are often given access to while investigating criminal activity.

Previously, law enforcement was limited to asynchronous methods in which a photograph or video-still would be entered into a computer program (Schuppe, 2018). Current technology has given law enforcement the capability to scan faces in crowded venues in real-time (Schuppe).

Thus far, U.S. police agencies have resisted incorporating this technology into practice, although departments such as the Los Angeles County Sheriff's Department are believed to possess the equipment necessary to bring this to fruition (Kaste, 2018).

Body worn cameras. On March 4th, 2020, Los Lunas Police Department in New Mexico entered into an agreement with Wolfcom to assist in beta-testing live facial recognition equipped body worn cameras (Gershgorn, 2020). According to Wolfcom CEO Peter Onruang, the company's body worn cameras could apply the facial recognition algorithms themselves or connect to a secondary system which would then run the algorithms (Westrope, 2020). Results of the beta testing were not available as officials with the Los Lunas Police Department refused comment (Gershgorn, 2020).

As Wolfcom pushes on in their quest to integrate FRT into their body worn cameras, Axon, the leading manufacturer in this industry, has paused efforts to incorporate face matching technology into their products (Ingber, 2019). According to Axon's artificial intelligence ethics board, limitations in face matching technology and ethical concerns over its use has resulted in the company not seeking to integrate these technologies into their cameras at this time (Smith, 2019). Axon does, however, utilize face detection technology for the purposes of streamlining face redaction and blurring out of faces in videos (Smith, 2019).

Reasons for and against. One of the more frequent arguments for equipping police officers with the capability of performing facial recognition in real-time has been the ability of officers to quickly identify members of the public they come in contact with (Castro & McLaughlin, 2019). Advocates state that the technology will assist in locating lost or missing children and help locate children exploited in human trafficking rings (Doffman, 2019). Some supporters even surmise that the technology will improve police accountability measures (Castro & McLaughlin, 2019).

Detractors often cite the lack of an individual's right not to participate in such a program, even equating the technology's use with a violation of the Fourth Amendment of the Constitution (Harwell, 2018). Other concerns include real-time FRT being used as a precursor to mass surveillance, which has recently been deployed in China (Ingber, 2019). Another main talking point of those skeptical of real-time FRT applications is the misidentification of subjects, especially women and minorities (EFF, 2017).

Federal Law Enforcement Applications

Multiple Federal Law Enforcement agencies implement FRT as an investigative tool. The prevailing agency, the FBI, has become the de-facto provider of FRT comparisons for other federal and local law enforcement (Gulliani, 2019).

Next Generation Identification system. In 2008, the FBI granted a contract worth \$1.1 billion dollars to Lockheed Martin for the creation and implementation of what is now referred to as the Next Generation Identification (NGI) system (Huffaker, 2016). According to a Lockheed Martin press release, the NGI is labeled as state-of-the-art biometric systems that was designed to improve the FBI's ability to "accurately and efficiently identify criminals" (Lockheed Martin, 2014). Released in four increments, the system came online in 2011, and in 2014 became fully operational

with the FBI receiving facial recognition capabilities with the addition of the Interstate Photo System (IPS) (Miller, 2015).

In 2019, data suggests that the FBI had access to over 640 million photographs in the IPS (Guliani, 2019). Lockheed Martin (2014) boasted that the NGI was made available to 18,000 law enforcement agencies across the country, courtesy of the FBI. Officials stated that during an 18-month timeframe between 2017 and 2019, the FBI's Facial Analysis, Comparison, and Evaluation (FACE) Services Unit received 152,565 requests from law enforcement agencies for facial identification purposes (Del Greco, 2019). In 2018, the FBI requested permission to upgrade their current algorithm software to one that claims a 99.12% Rank 1 accuracy, meaning that the first photo the algorithm produced was a correct match over 99% of the time (Del Greco, 2019).

The NGI is designed to accept a probe photo, or photo of an individual that law enforcement officials are seeking to identify (CRS, 2020). The probe photo is then entered into the NGI-IPS, at which time target photos are returned based on the parameters of the threshold, or similarity score (CRS, 2020). The threshold for the NGI is defaulted to twenty pictures unless adjusted but is capable of returning up to fifty target photos (FBI, 2019).

According to the NGI Policy and Implementation Guide (2019), The FBI has included several requirements to those agencies looking to take advantage of the NGI-IPS:

- The submission of photographs of individuals practicing their rights guaranteed under the First Amendment are strictly prohibited.
- Candidate photos returned to law enforcement officials are provided as investigatory leads and not to be thought of as a positive identification.
- Law enforcement agency users must have completed facial recognition training in compliance with scientific national standards, prior to conducting facial recognition searches.
- It is the responsibility of the law enforcement agency to create their own facial recognition use policy prior to using the NGI-IPS.
- The probe photo is not retained upon completion of the FRT process.

Applications by federal agencies. FRT programs are utilized by nearly all agencies within the federal law enforcement community. The Department of Homeland Security (DHS) and the Customs and Border Patrol (CBP) currently employ FRT at 27 of the nation's airports (GAO(b), 2020). International travelers arriving at 15 airports have their photograph taken while at the Customs inspection booth, which is then compared to passport or visa photos (Street, 2019). In addition, 22 airports are equipped with biometric exit technology. As international travelers leave the United States the CBP creates a gallery of images from each traveler aboard an aircraft, which is then compared to a photograph of the passenger at the boarding gate (Street, 2019). According to the Transportation Security Administration (TSA), of the more than 19 million passengers screened via facial recognition programs, 100 people were identified as not matching the identification presented at security checkpoints (Taylor, n.d.).

FRT programs are also active at United States border crossings. CBP agents scan the faces of thousands of pedestrians at border crossings each day. U.S. citizens may opt out of this process, if notification is made to a Customs agent and a request is made for a manual documentation check (CBP(b), 2020). CBP officials state that the use of FRT is a result of the direct recommendation from the 9/11 commission; as of 2020, 262 persons have been caught using fraudulent paperwork (CBP(a), 2020).

Immigration and Customs Enforcement (ICE) stated that the use of FRT is primarily to assist the agency with human trafficking, child exploitation, online sexual exploitation of children, identity fraud, and identification of members of transnational criminal organizations (DHS, 2020). ICE officials have also come under scrutiny for their use of FRT on DMV driver's licenses in attempts to identify and locate persons residing in the U.S. illegally (LeBlanc, 2019). Critics of this policy argue that ICE does not obtain court orders or warrants to request information from DMVs, but rather an administrative subpoena (Chapell, 2019).

Current Law

Federal statutes. To date there are no federal laws governing the use of FRT by federal law enforcement agencies (Greenberg, 2020). However, 2020 saw the introduction of two bills brought to the Senate floor seeking to regulate the use of FRT, not only by law enforcement, but also in the private sector. In February 2020, Senator Jeff Merkley, a democrat from Oregon, introduced the Ethical Use of Facial Recognition Act (S.3284 -116th Congress: 2020). Language in this proposal stated:

- Facial recognition is a technology that is increasingly being used and marketed to law enforcement agencies across the United States without appropriate debate or consideration of its impacts.
- Facial recognition has been shown to disproportionately impact communities of color, activists, immigrants, and other groups that are often already unjustly targeted.
- Facial recognition has a history of being inaccurate, particularly for women, young people, African Americans, and other ethnic groups.
- There is evidence that facial recognition has been used at protests and rallies, which could hinder First Amendment protected free speech.
- It is critical that facial recognition not be used to suppress First Amendment related activities, violate privacy, or otherwise adversely impact individuals' civil rights and civil liberties.

This bill included provisions prohibiting law enforcement officials from utilizing FRT prior to securing a search warrant (S.3284 -116th Congress: 2020). In addition, the legislation threatened to withhold federal public safety grants to local and state governments that engaged in biometric

surveillance (S. 3284-116th Congress: 2020). Finally, the Ethical Use of Facial Recognition Act (2020), sought to establish a commission to create guidelines on the use of FRT. The bill was read twice and then referred to the Committee on Homeland Security and Governmental Affairs.

A second piece of legislation proposed by Senator Merkley titled The National Biometric Information Privacy Act (2020) proposed a prohibition on the collection of biometric surveillance from private entities. The bill stated that private entities were prohibited from sharing biometric data with law enforcement agencies absent a warrant (S. 4400-116th Congress: 2020). Other provisions in this bill included:

- Mandates that any entity in possession of biometric data authored a written policy establishing retention schedules
- Biometric data must be destroyed 1 year after a person's last interaction with the entity
- Establishes guidelines on the circumstances in which a private entity may collect biometric information
- Prohibits the selling of biometric data for profit without the written consent of the affected individual
- Any biometric data collected in violation of this act would become inadmissible in criminal, civil, administrative, or other investigation or proceeding.

The bill, co-sponsored by Senator Bernie Sanders, was introduced to Congress on August 3rd, 2020, but did not receive a vote (S. 4400-116th Congress: National Biometric Information Privacy Act of 2020). Senator Sanders, who is a staunch opponent of FRT, stated in preparation for his 2020 presidential bid that he would prefer to ban law enforcement from utilizing any algorithmic assessment tools (O'Sullivan, 2019).

State legislation. While some states have enacted legislation to protect consumers from commercial use of FRT, only the state of Washington incorporates a comprehensive list of regulations on FRT applications used by law enforcement agencies (Greenberg, 2020). Chapter 43.386 of the Revised Code of Washington, Senate Bill 6280, (2020), employs stringent restrictions on state and local government's use of FRT. The bulk of this law delineates the specific requirements regarding the process of procuring FRT software, training standards, and reporting (S.B. 6280, 66th Legislature, WA. 2020).

According to Bill 6280 (2020), law enforcement agencies are required to notify defendants of the use of FRT prior to the start of trial. Agencies are also mandated to maintain sufficient records involving the use of FRT in order to facilitate compliance audits (S.B. 6280, 66th Legislature, WA. 2020). On an annual basis, agencies must also disclose non-identifying demographic information for individuals for whom a warrant was applied or obtained to conduct surveillance through FRT applications (S.B. 6280, 66th Legislature, WA. 2020).

Several prohibitions in Bill 6280 (2020) included:

- FRT is not allowed to conduct real-time identification or persistent tracking absent exigent circumstances or without obtaining a valid warrant;
- FRT is forbidden to be used on individuals based on race, religion, political views or activities, gender, and other factors;
- Agencies may not use FRT to create a record of individuals for the purposes of describing acts being practiced that are protected under the First Amendment of the Constitution;
- FRT cannot be the sole basis of probable cause in a criminal investigation.

The bill was passed by the State of Washington House of Representatives in March 2020 by a vote of 53-43. Later that same day the state Senate ratified the bill 27-21 (S.B. 6280, 66th Legislature, WA. 2020). Bill 6280 was signed into law by Governor Jay Inslee with an effective date of July 1st, 2021 (S.B. 6280, 66th Legislature, WA. 2020).

Additionally, the State of Massachusetts passed "An Act Relative to Justice, Equity, and Accountability in Law Enforcement in the Commonwealth," on December 31, 2020. The act specified that law enforcement agencies in the state may request facial recognition searches from the state's department of motor vehicles (S.2963, 192nd General Court, MA, 2020). Searches may only be performed after officers obtain a warrant issued by a justice of the superior court, based on probable cause that the results of FRT will lead to evidence of a violent felony offense (S.2963, 192nd General Court, MA, 2020). A search may be conducted absent a warrant if exigent circumstances are present. However, FRT searches conducted without a warrant require a sworn affidavit from a supervisory official within 48 hours detailing the necessity to conduct said search and the exigent circumstances that were present (S.2963, 192nd General Court, MA, 2020).

Other states such as California, New Hampshire, and Oregon have passed legislation on the incorporation of FRT software on body worn cameras (Greenberg, 2020). California's Law enforcement: facial recognition and biometric surveillance laws (2019) prohibit agencies from "installing, activating, or using any biometric surveillance in connection with an officer's camera," (A.B. 1215, 2019-20 Reg. Sess, CA. 2019). New Hampshire law states the officers may not utilize video recordings captured from body worn cameras for the purposes of entering said footage into FRT software, although officers may use still captured images from body worn camera footage in order to identify subjects believed to have involvement in a crime (NH Rev Stat § 105-D:2 (2016)). Oregon state law strictly prohibits agencies from applying FRT to videos obtained through body worn cameras (ORS § 133.741). An additional 18 state legislative bodies have proposed limiting the ability of law enforcement and government agencies biometric data collection abilities (Greenberg, 2019).

Local ordinances. Several major metropolitan cities severely limit or outright ban local police departments from the use of FRT. Cities including Minneapolis and New York are debating facial recognition bans (Jany, 2021; Hern, 2021). A number of these local ordinances forbid FRT usage by law enforcement officials, but private businesses and civilians are granted certain exceptions to the collection of biometric data for the purpose of facial recognition (Jany, 2021).

The following list includes a selection of city ordinances and summarizes some of their provisions:

San Francisco, California: Heavily restricts the ability for city agencies to procure and/or use FRT applications (San Francisco, California, Administrative Code sec. 19B § Acquisition of Surveillance Technology, 2019). At the time of the bill's passage, the San Francisco Police Department did not possess the capability or have the equipment to conduct facial recognition surveillance (Conger et al., 2019).

Boston, Massachusetts: The Ordinance Banning Face Surveillance Technology in Boston (2020), makes it unlawful for an official from the City of Boston to obtain, retain, possess, access, or use any facial recognition system. Officials are also prohibited from requesting or authorizing a third party to access a facial recognition system on their behalf (Boston, Massachusetts, City Ordinance 16-62 § Ordinance Banning Face Surveillance Technology in Boston, 2020).

However, according to Ordinance 16-62 (2020), members are allowed to present evidence from a specific crime in which FRT was utilized, as long as no official from Boston generated or requested said evidence. Furthermore, any evidence obtained in violation of this directive will be inadmissible in court (Boston, Massachusetts, 2020). Any employee found in violation of this ordinance is subject to retraining, suspension, or termination.

Portland, Oregon: In January of 2021, the city of Portland, Oregon, passed city ordinance 190114, titled Digital Justice (2021). This ordinance prevents any governmental agency and private entities from utilizing FRT. The ordinance includes a provision to allow private entities to incorporate FRT on a limited basis, but they are not allowed to employ the technology in areas considered public accommodations (Portland, Oregon, Ordinance 190114, Code Title 34 § Digital Justice (2021). Private entities found in violation of the ordinance are susceptible to civil litigation, in which a plaintiff may be awarded up to \$1,000 a day (Portland, Oregon, 2021).

Portland, Maine: In 2020, Portland, Maine residents passed Ordinance 72 -19/20 (2020), by referendum. The Facial Recognition Technology ordinance prohibits any employee from the city of Portland to obtain, retain, store, possess, access, use, or collect any facial recognition surveillance tool, or to enter into a third-party agreement for this purpose (Portland, Maine, Ord. 72-19/20 § Article XI. Facial Recognition Technology, 2020). Similar to Portland, Oregon, persons deemed harmed by failure to follow this act are subject to relief of up to \$1,000 per day (Portland, Maine, 2020). Employees found in violation of this ordinance are subject to discipline including termination (Portland, Maine, 2020).

Current Legal Challenges

The use of FRT in criminal cases is a rather novel subject. It is believed that as the technology advances and becomes more reliable, FRT will become more prominent in criminal prosecutions. Scholars agree that sometime in the near-future prosecutors will seek to present evidence recovered from FRT applications to establish probable cause or defendant identification (Hamann & Smith, 2019). To date, litigation from within the judicial system as to the legality of this technology and its lawfulness to be accepted as evidence in a court of law has been scarce. Below is a list of cases in the judicial system and their possible impacts upon FRT.

Lynch v. State. On September 12th, 2015, two undercover Jacksonville police officers purchased \$50 of crack cocaine from an unknown individual referred to as "Midnight" (Brown, 2019). Officers were able to capture cell phone photos of "Midnight" before leaving the scene without making an arrest (*Lynch v. State*, 260 So. 3d 1166 Fla. Dist. Ct. App. 2018). Officers then sent the photos to a crime analyst for identification (*Lynch v. State*, 2018). The analyst testified in pre-trial motions that after attempting to identify "Midnight" through other police databases, a cell phone capture was uploaded into a facial recognition program (*Lynch v. State*, 2018). The program returned Willie Lynch as the highest-rated match; however, the program only assigned the likelihood of a match at one star, or one of the lowest possible rating matches (*Lynch v. State*, 2018). Nonetheless, the analyst produced the photograph to the officers who then made a positive identification (*Lynch v. State*, 2018).

Willie Lynch was subsequently found guilty in a jury trial and sentenced to eight years in prison (*Lynch v. State*, 2018). On appeal Lynch argued that he should have had access to the other photographs produced by the FRT program. Lynch surmised that the prosecution violated *Brady v. Maryland*, 373 U.S. 83 (1963) by not presenting the defense with these photographs (*Lynch v. State*, 2018). This motion was denied unanimously, as the decision stated that Lynch failed to prove that the other photos returned from the program resembled him, and that the jury convicted Lynch after comparing the photographs that the officers took from the cellphone camera with the photograph returned by the FRT program (*Lynch v. State*, 2018).

People v. Reyes. On September 29th, 2019, Luis Reyes allegedly committed a burglary in New York City (*People v. Reyes*, N.Y. Slip Op. 20258, N.Y. Sup. Ct. 2020). Detectives submitted still photographs captured from surveillance camera footage during the crime into the NYPD's FRT program (*People v. Reyes*, 2020). FRT software returned one possible match, which was that of defendant (*People v. Reyes*, 2020). Detectives then compared numerous other booking photos of Reyes to the stills retrieved from the surveillance footage (*People v. Reyes*, 2020). Police were also able to match tattoos from Reyes' booking photographs to those found on the suspect in the video surveillance footage, determining that the suspect in the videos was indeed Luis Reyes (*People v. Reyes*, 2020).

On appeal, Reyes challenged the police officers' viewing of the surveillance video as a product of the identification process (*People v. Reyes*, 2020). The court ruled that *People v. Gee* was not relevant to this case, as the "detective was not resolving whether the person in the video was the one who committed the burglary; that was a given. He looked at the video to determine whether he knew someone in it" (*People v. Reyes*, 2020).

Justice Mark Dwyer wrote in his opinion the following regarding facial recognition (2020):

To the best of this judge's knowledge, a facial recognition "match" has never been admitted at a New York criminal trial as evidence that an unknown person in one photo is the known person in another. There is no agreement in a relevant community of technological experts that matches are sufficiently reliable to be used in court as identification evidence. *See Frye v. United States*, 293 F 1013 (D.C. Cir 1923). Facial recognition analysis thus joins a growing number of scientific and near-scientific techniques that may be used as tools for identifying or eliminating suspects, but that do not produce results admissible at a

trial. *Cf. People v. Williams*, 35 NY3d 24, 43-44 (2020). The People argue that the [FRT] results were just of this sort, and can provide investigative leads.

Furthermore, Justice Dwyer wrote in his decision regarding Reyes' request for appeal of the discovery of FRT software in this case: "No reason appears for the judicial invention of a suppression doctrine in these circumstances. Nor is there any reason for discovery about facial recognition software that was used as a simple trigger for investigation and will presumably not be the basis for testimony at a trial" (*People v. Reyes*, 2020).

Confrontation Clause. The Sixth Amendment of the U.S. Constitution guarantees specific rights to defendants in criminal cases. The Confrontation Clause within the Sixth Amendment specifies that the accused shall enjoy the right to confront the witnesses against them (U.S. Const. amend. VI). The Confrontation Clause was first argued in the U.S. Supreme Court in 1895. In *Mattox v. U.S.* (1895), Justice Henry Billings Brown opined:

The primary object of the constitutional provision in question was to prevent depositions or ex parte affidavits, such as were sometimes admitted in civil cases, being used against the prisoner in lieu of a personal examination and cross-examination of the witness, in which the accused has an opportunity, not only of testing the recollection and sifting the conscience of the witness, but of compelling him to stand face to face with the jury in order that they may look at him, and judge by his demeanor upon the stand and the manner in which he gives his testimony whether he is worthy of belief (*Mattox v. United States*, 156 U.S. 237, 242-43, 1895).

The interpretation of this clause has gone through numerous iterations since *Mattox v. United States* (1895), but courts have not yet ruled on the proper application of this rule to machine accusers, even those assisted by a human element (Sites, 2020).

Issues with Confrontation Clause. In *Ohio v. Roberts* (1980), the Honorable Judge Brennan wrote in his dissent that evidence or testimony could be presented at trial without the testimony of the witness at trial, assuming that the testimony bore sufficient "indicia of reliability," meaning that the evidence or testimony passed a test to determine that it was reliable and trustworthy (*Ohio v. Roberts*, 448 U.S. 56, 100 S. Ct. 2531, 1980). *Crawford v. Washington* (2004) altered the test of admissibility under the Confrontation Clause, stating that absent witness statements are not admissible (*Crawford v. Washington*, 541 U.S. 36, 124 S. Ct. 1354, 2004). *Whorton v. Bockting* (2007) subsequently ruled that the Confrontation Clause does not apply to nontestimonial out-of-court statements (*Whorton v. Bockting*, 549 U.S. 406, 127 S. Ct. 1173, 2007). Courts are now required to determine if a specific statement is testimonial but have failed to clearly define the term "testimonial" (Celentino, 2016). Furthermore, the only exception to the clause occurs when the defendant had a prior opportunity to cross-examine said witness (*Crawford v. Washington*, 2004).

Current legal precedent fails to clearly define the admissibility of evidence recovered from FRT applications. In *Williams v. Illinois* (2012) Justice Alito wrote that a defendant's rights to the Confrontation Clause are not violated if the State provides an expert witness to testify to their opinion on reports completed by non-testifying analysts (*Williams v. Illinois*, 567 U.S. 50, 132 S. Ct. 2221, 183 L. Ed. 2d 89, 23 Fla. L. Weekly Supp. 355, 2012). In *State v. Ortiz-Zape* (2013) the courts have ruled that machine-generated raw data is not considered testimonial evidence (*State v.*

Ortiz-Zape, 743 S.E.2d 156, 367 N.C. 1, N.C. 2013). If the data produced by the machine is reasonably deemed reliable by experts, then the information may be disclosed at trial (Smith, 2015). On the contrary, a non-testifying analyst's opinion that is derived from machine-generated data is considered testimonial, meaning that the raw data is admissible, but the analyst's conclusion regarding said data will not be (Smith, 2015).

Hearsay rule. According to Rule 801 of The Federal Rules of Evidence (2014), hearsay is defined as a statement that: "(1) the declarant does not make while testifying at the current trial or hearing; and (2) a party offers in evidence to prove the truth of the matter asserted in the statement," (United States, 2014). While there are exceptions to the rule, typically hearsay is not allowed to be entered into evidence. The Federal Rules of Evidence fails to declare if machines should be considered declarants under the Hearsay Rule and subject to the Confrontation Clause (Crossey, 2020).

Issues with Hearsay rule. Due to the uncertainty of the manner in which evidence obtained from FRT applications will be viewed by the court, it is unknown if the Confrontation Clause or Hearsay rule will become applicable. According to *Bullcoming v. New Mexico* (2011), forensic reports are testimonial and therefore the analyst who performed the certification must be made available to testify (*Bullcoming v. New Mexico*, 131 S. Ct. 2705, 2717, 2011). If FRT is deemed testimonial, prosecutors will have to produce the analyst who performed the comparison and certified the results of a facial recognition search in a court of law.

The Hearsay requirement only applies if the evidence is being submitted to “prove the truth of the matter herein” (Celentino, 2016, p. 1318). In *Williams v. Illinois* (2012), prosecutors did not attempt to enter a DNA report itself on defendant Williams, instead offering an expert witness who testified that Williams’ DNA was a match to that of the DNA in the report (*Williams v. Illinois*, 2012). The Supreme Court ruled that the Confrontation Clause, and by default the Hearsay rule, did not apply to this case.

Justice Samuel Alito, in concurrence with Justice Kennedy and Justice Breyer, wrote the following in his opinion (2012):

We also conclude that even if the [DNA report] had been admitted into evidence, there would have been no Confrontation Clause violation. The [DNA report] is very different from the sort of extrajudicial statements... that the Confrontation Clause was originally understood to reach. The report was produced before any suspect was identified. The report was sought not for the purpose of obtaining evidence to be used against petitioner, who was not even under suspicion at the time, but for the purpose of finding a rapist who was on the loose. (*Williams v. Illinois*, 2012).

This might lead one to believe that if FRT was performed for the purposes of identifying an unknown subject, rather than to confirm an identity, then the results would not be applicable to the Hearsay rule or Confrontation Clause.

Fourth Amendment. This amendment secures a person's right from unreasonable searches by government officials absent the obtainment of a warrant showing probable cause (U.S. Const. amend. IV). Scholars have argued the legalities of applying real-time FRT in public spaces bringing forth arguments related to the Fourth Amendment (Lochner, 2013). Two court rulings are

employed to determine if an act constitutes a search: *Katz v. United States*, a reasonable expectation of privacy test, and *Jones v. United States*, a trespass test (Lochner, 2013). In *Katz* (1967), the courts ruled that if a person exhibits a subjective expectation of privacy and a reasonable person would agree, interference by law enforcement would constitute as a search (*Katz v. United States*, 389 U.S. 347, 88 S. Ct. 507, 1967). In *Jones* (2012), the court ruled that persons have no reasonable expectation to privacy to data they volunteered to a third-party company, so long as that company maintained said data over the normal course of business (*United States v. Jones*, 908 F. Supp. 2d 203 (D.D.C. 2012)).

A technology utilized by law enforcement agencies, Automated License Plate Readers (ALPR), have parallel legal challenges. ALPRs are the combination of fast processing computers equipped with image processing technology that convert data, which can be compared with databases containing license plate information (Greenberg, 2015). Law enforcement agencies mount ALPRs to police vehicles or in fixed locations. As vehicles pass an ALPR, a camera takes a picture of the license plate and converts the data, which then can reveal information such as if the vehicle is stolen, or the registered owner has a warrant (Greenberg, 2015).

As no court has opined the legalities of ALPR usage, two doctrines have typically been applied. In *New York v. Class* (1986), the courts ruled that due to "the pervasive governmental regulations of automobiles," the operator of a motor vehicle can expect to have some levels of privacy infringed upon by the state (*New York v. Class*, 475 U.S. 106, 113, 1986). The second doctrine, *United States v. Knotts* (1983), found that persons traveling in a vehicle have no expectation to privacy, as their movement could be observed by any member of the public with the naked eye (*United States v. Knotts*, 460 U.S. 276, 280, 1983).

It is assumed that people walking down the street enjoy greater protections under the Fourth Amendment than automobiles traveling down the roadway. As stated in *Katz v. United States* (1967), the Fourth Amendment "protects people, not places" (*Katz v. United States*, 1967). Clare Garvie, a Georgetown law professor, highlighted the legal challenges of incorporating real-time FRT into body worn cameras. Garvie noted that no notice is given to persons subjected to this technology, no consent is asked or given by said persons, and no probable cause exists to conduct a facial recognition search in the first place (Stroud, 2016).

Conversely, under *Olmstead v. United States* (1928), justices argued that visual surveillance does not constitute a search (*Olmstead v. United States*, 277 U.S. 438, 48 S. Ct. 564, 1928). A recent study found that the average American is recorded on some type of camera 34 times a day (Brainard, 2020). If a person is cognizant of the fact that they are appearing on hundreds of cameras a week, how much privacy do they expect to enjoy? An argument then arises, to what extent is visual surveillance by law enforcement utilizing FRT software considered a search in violation of the Fourth Amendment?

Methodology

Conceptual Framework

There are two theories that I will adopt for the purposes of this study: group theory and technology acceptance theory. Utilizing these conceptual frameworks established the basis of this study in its theories, concepts, and practical contexts. Also, these theories assisted in identifying the implications of the study, situating my identity and positionality, and articulating how these aspects are interrelated in reference to methodological frames and processes (Ravitch & Carl, 2015).

Group theory analyzes how the various groups within a society attempt to influence public policy formulation to their advantage (Anyebe, 2018). Public policy is seen as a compromise among different interest groups, often favoring the most powerful political group at that particular point in history (Anyebe, 2018). The foremost tenet of group theory is the need for access to decision-makers (Anderson, 2003).

Upon completion of this research project, several groups, or stakeholders, will be relevant in developing a FRT policy. They include: law enforcement officials, legislators, the population at large, developers of FRT technology, and members of the legal profession. Input and perspective from all the above groups will become paramount in the acceptance of the legitimacy of a FRT policy.

Technology acceptance theory, more specifically the combined technology acceptance model (C-TAM-TPB), is a combination of the technology acceptance model (TAM) and theory of planned behavior (TPB). This theory examines the relationship between a user's adoption of technology and the factors that determine their acceptance of it (Taherdoost, 2017). Taylor and Todd (1995) combined the advantages of perceived usefulness and perceived ease of use found in TAM with perceived behavioral control found in TPB.

For FRT technology to become accepted on a larger scale than it currently enjoys, it will be important for the general public to understand the usefulness of FRT with at least the perception of controlling the methods in which FRT is employed. This will require law enforcement departments to become proactive with the positive capabilities afforded by facial recognition technology.

Rationale for Research Tradition

This research was a non-experimental collective case study design informed by constructivist data analysis methods. This design was prudent for this study as this research project involved variables that were not manipulated, and the research setting was not controlled (Patidar, 2013).

A case study approach allows for a comprehensive examination of intricate and often hot-topic issues in a real-life context (Crowe, et al., 2011). This particular approach is well recognized in research involving legal doctrine and policy creation (Crowe, et al., 2011). This researcher believes

that conducting the study in this manner highlighted the most critical and relevant solutions for creating a FRT policy.

Literature Search Strategies

Literature was discovered utilizing the DePaul University Library, DePaul University's Rinn Law Library, as well as other search engines. Search terms such as facial recognition technology, facial recognition legislature, police department facial recognition policy, legal challenges of facial recognition, and others were entered into ProQuest, Google Scholar, and Google. In addition, information was gathered from peer-reviewed scholarly journals, law-review articles, newspaper articles, blogs, magazine articles, and books. The material consisted mainly of works published between 2000 and 2020, as FRT utilization by law enforcement agencies and the legislation governing its use is a recent and evolving phenomenon.

Data Collection

This research project was completed through the collection and analysis of primary and secondary document data review.

Document Review

The document research included primary and secondary data. Secondary data was collected from peer-reviewed journal articles, governmental publications, law review articles, newspaper articles, blogs, magazine articles, and books. The material covering FRT consisted mainly of works published between the years 2010 and 2020. A portion of the material dates to the early 1900s and through the 20th century when referencing prior court decisions involving the usage of technologies such as fingerprints and DNA. The timeframe parameters and sources of information were selected because facial recognition technology is a relatively recent tool utilized by law enforcement agencies. Due to the rapid evolution of FRT, new studies will continue to be published, limiting the researcher's ability to conduct a comprehensive scholarly review for this project.

The data collected were analyzed to inform a policy that will include the best practices found for implementing a FRT policy by a law enforcement agency. In addition to this secondary source data, primary source data in the form of FRT policies were collected and studied. These data were also analyzed to identify issues and emerging themes that answered the research questions.

The information gleaned from this research was applied in the creation of recommendations for an FRT policy that adheres to the best practices in the law enforcement community. Finally, federal, state, and local laws were examined to ensure that the recommendations adhere to federal provisions. The outline for these policy recommendations is general enough to allow for an individual agency to edit it so as to comply with with relevant state and local provisions.

Data Analysis Methods

To complete the project, this researcher created several unique datasets. One dataset consisted of previously discussed, commonly accepted technologies such as fingerprints and DNA. It provided a historical timeline of their introduction to the law enforcement community and the path required to become routinely accepted scientifically sound evidence in court proceedings. Three datasets were created to highlight the similarities and differences of critical court rulings that will have an effect on FRT in the future. An additional dataset examined FRT policies made available to the public through open-source searches of the forty largest municipal police departments and ten largest sheriff's offices in the country. When available, these policies were examined at length. Finally, certain information from these datasets was cross-referenced to create a FRT policy that will be applicable to a large portion of law enforcement agencies within the United States.

Comparative law review. The purpose of conducting a comparative law review is to understand the role of law and to promote a common understanding of critical issues (Eberle, 2009). One of the guiding principles when conducting a comparative law review is to make explicit comparisons in legal doctrines' similarities and differences (Reitz, 1998). Comparative law studies have the ability to focus on core constitutional principles such as the right to privacy and protections from illegal search and seizures (Eberle, 2009). According to Reitz (1998) a comparative law study devotes substantial efforts to explore the functional equivalents, or lack thereof, in the aspect under study.

This method has been used in studies by policy-makers and legislators to aid in law reform and policy development (Paris, 2016). Andenas and Fairgrieve (2012) wrote that this methodology is relevant when a researcher is studying a particular legal issue in which a hypothesis is being tested to achieve an expected outcome and to advance knowledge on that issue. This methodology is prudent when the researcher is proposing solutions from a policy-based perspective, in particular policy frameworks or best practices relating to the creation of policy (Paris, 2016).

This study concluded with an internal comparison of the U.S. legal system focused on the commonly accepted technologies of fingerprints and deoxyribonucleic acid (DNA) in criminal proceedings. This research details the history of technologies currently accepted into criminal proceedings and deemed reliable as to their effectiveness. Fingerprint and DNA technology are often given little debate about their reliability, but this has not always been the case. To complete this section, the legal history of these two technologies is briefly explained. Beginning with their introduction into criminal cases, through recent legal challenges, court cases are presented with the resulting ruling of the courts given.

More specifically, this study focuses on legal challenges to admissibility, the Confrontation Clause, the Hearsay Rule, and the Fourth Amendment of the above-mentioned technologies. The researcher explored the similarities and differences in legal challenges as these technologies navigated the criminal justice system to become widely recognized as reliable and effective. Two separate tables have been created that highlight the dominant similarities and differences. The results from this comparison review were used as the basis for the researcher's assumptions about future legal challenges to FRT.

While no consensus exists governing the process in which a comparative law review should be conducted, this researcher employed a three-part strategy suggested by W.J. Kamba (Kamba, 1974; Paris, 2016).

1. Descriptive Phase - explains the legal concepts of the technologies and the legal solutions provided by these court rulings.
2. Identification Phase - Identify the similarities and differences between the court rulings regarding these court rulings.
3. Explanatory Phase - Provide an account for these similarities and differences and hypothesize the effects that may await FRT.

Steps one and two are discussed in the results phase of this research paper, while step three is presented in the discussion section of this project.

This strategy was implemented following three core principle rules set forth by Eberle (2009):

- Step # 1 - Evaluate the law as it is expressed concretely. The court rulings were evaluated in order to understand the context of the ruling and how this ruling is applied to fingerprint and DNA technology.
- Step # 2 - Evaluate how the law actually operates within a culture. This includes interpretations of the law and their direct effect on statutes, policies, and regulations imposed by government officials. Focus on the internal dimension of the law, or implicit patterns, to fully understand how the law operates within the culture of criminal court proceedings and technology.
- Step 3 - Assemble the results of the study and determine what legal data points will be focused on. These data points will be the basis of answering the questions: What have we learned? What are the trends and patterns of these rulings? Will these data points allow for extrapolation to best determine the future path of FRT?

Policy evaluation. To obtain the policies needed for evaluation, this researcher conducted an open-source inquiry into the 40 largest municipal police departments and ten largest county sheriff's offices by sworn personnel in the United States. Once the departments included in this study were determined, the researcher conducted an open-source inquiry to determine if a department had a publicly viewable policy or directive governing the use of FRT. The researcher visited the department's official website and determined if it directs visitors to their list of policies or directives. If the policies/directives could be located, a search of the documents revealed if a FRT policy exists. If a policy was found, it was downloaded for further examination.

While locating these policies, another search was conducted concurrently to determine if the department has publicly acknowledged or denied the existence of an FRT program. The author then attempted to locate information pertaining if said department had previously utilized FRT but is currently forbidden due to local or state legislation.

In addition to the three previously mentioned documents that were used to create a sample policy, the policy evaluation utilized "Measuring Excellence: Planning and Managing Evaluations of Law Enforcement Initiatives." This document was authored by the Inner City Fund (ICF) International in cooperation with the Office of Community Oriented Policing Services, U.S. Department of Justice. The primary objective of this research was to provide the information necessary for a law enforcement agency to conduct and manage program evaluations (Ward et al., 2007). According to the authors, a program evaluation is defined "as a systematic process of gathering and analyzing information for the purposes of program assessment, program improvement, and, in a broader sense, strategic management" (Ward et al., 2007, p. 3).

There are several advantages to conducting an evaluation of a program in a law enforcement agency. Chibnall et al. (2007) surmised that program evaluations are essential for cutting-edge policing approaches, such as those found in a FRT program. Furthermore, incorporating stakeholder participation offers an invaluable opportunity for program enhancement and improvement (Chibnall et al., 2007). Stakeholder participation will lead to increased credibility, buy-in, partnership, and accountability, which tends to increase citizen satisfaction (Chibnall et al., 2007).

To conduct this FRT policy evaluation, this researcher has created a hybrid evaluation model that examines the process, outcome, and impact of the policy. The purpose of this study process refers to the actions or steps taken by department members when operating a FRT program. The outcome references the goals and objectives desired in utilizing a FRT program. Lastly, the researcher examined the effects that a FRT program desires to change.

Below is a list of the aims that each of these evaluations attempted to address:

Process

- The steps needed to collect, submit, and analyze target and sample photographs.
- Number and content of training session topics.
- Roles and responsibilities of each member involved in the program.

Outcome

- Increase in the number of arrests of criminals.
- Increase in the number of cases closed with an arrest and prosecution.
- Improved methods of locating lost / missing / exploited children.

Impact

- Increase in public perception of credibility.
- Decrease in felony cases that go unsolved.

Below is a list of the variables that were examined pertaining to the individual FRT policies that have been collected. Each variable is listed with a brief description as to the definition that will be used to evaluate each policy. Each document was examined to determine if said element is present in the policy. The table below illustrates whether the individual policy incorporates said element: “yes” is indicated if the particular issue is discussed in the document and "no" if it is not addressed.

- *Describes the process of FRT*- Describes the process for collecting/submitting images for comparison, the process for evaluating returned images, and related information applicable to the use of FRT.
- *Limits the scope of utilization* - Describes the actions that would allow or prohibit a member from utilizing FRT.
- *Oversight process* - Details procedures in which supervisors monitor FRT programs to ensure accuracy and compliance with existing laws and policies.
- *Training program* - Describes a training regimen that FRT operators and requesters undergo prior to FRT usage.
- *Verification mechanisms* - Describes in detail the process in which returned images can be considered a match for the target image based on similarity score.
- *Record keeping standards* - Defines the process for FRT usage, including how requests, submissions, and returned images are stored and the process through which those records would be made available to the public.

After examining each policy, the researcher then decided if each individual policy possessed the above elements. If the element was found in the policy, a "yes" was placed for the category; if not, the box was marked "no." Below is a template of the table that was created upon completion of the study.

Figure 2. Example of Policy Evaluation Template

Police Department	Describes Process	Limits Scope	Oversight Process	Training Program	Verification Mechanisms	Record Keeping
--------------------------	--------------------------	---------------------	--------------------------	-------------------------	--------------------------------	-----------------------

Policy creation. In order to create a policy template for a FRT program, this author referred to three outside sources. The first was a best practice guide that was developed by the International Association of Chiefs of Police (IACP). This guide was created to assist in the creation and implementation of policy-procedure manuals. The second guide is a white paper authored by the World Economic Forum (WEF). This publication serves as a framework for responsible usage of FRT programs by law enforcement agency. Lastly, the researcher examined the Face Recognition Policy Template released by the Department of Justice (DOJ). In conjunction with the aforementioned manuals, this researcher examined the collected FRT policies to ascertain the most appropriate samples that will lead to a policy that offers the industry’s accepted best practices.

Court precedent was incorporated in drafting this policy template. The researcher also took into account the history of past technologies, such as fingerprints and DNA admissibility in court, and made recommendations based on the path FRT is most likely to follow in the future. As FRT court rulings are limited at this point, any recommendations should be considered as this author's best attempt at predicting future challenges to FRT. The resulting policy recommendations are generalized in regard to local and state laws, many of which will implement stricter limitations and regulations than will be accounted for in this template.

According to the IACP, a policy for a law enforcement agency should be: comprehensive providing direction and guidance, clearly written and easy to use, and consistent with the agency's organizational philosophy, legal requirements, and applicable standards (Orrick, n.d.). Additionally, Orrick (n.d.), states that the policy should be considered a living document that is reviewed and updated on a regular basis. Finally, the policy should incorporate and reflect accepted state and national best practices (Orrick, n.d.).

The WEF organized a community of forty-two individuals from technology companies, governmental organizations, and members of the academic community with the intention of creating a policy framework that defines "what constitutes the responsible use of facial recognition [by law enforcement agencies]" (WEF, 2021). This framework involves incorporating nine principles for law enforcement investigations. Following are brief summaries of the nine principles (WEF, 2021):

1. *Respect for human and fundamental rights* - FRT should only be used as part of lawful criminal investigations, and the individual rights of the subject should be respected at all times.
2. *Necessary and proportional use* - the decision to utilize FRT should be balanced between the need to identify a subject and the rights of the individual. Use of real-time FRT and the usage of publicly available photographs should be regulated and only used in very specific circumstances.
3. *Transparency* - law enforcement agencies should be forthcoming regarding FRT usage, vendors, and databases.
4. *Human oversight and accountability* - delineates that agencies should never issue an analysis and conclusion without the interpretation of a skilled facial examiner. These analyses shall be confirmed by blind verification or a second expert facial examiner before any law enforcement action is taken.
5. *System performance* - law enforcement agencies should follow specific standards to ensure accuracy of the algorithms designed by their vendors, and ensure vendors submit their algorithms for independent testing.
6. *Risk mitigation strategies* - should deploy risk mitigation processes to identify, monitor, and mitigate the risks of error and biases throughout the entire life cycle of the system.

7. *Training of facial examiners* - describes the importance of a training program that is consistently evaluated and updated to ensure examiners understand the capabilities and limitations of FRT.
8. *Use of probe images and reference databases* - collection of probe images should be conducted on a legal basis and maintained with a strict and transparent chain of custody procedure.
9. *Image and metadata integrity* - To mitigate the risk of errors, agencies should follow the recommendations of standards of photo quality collected for investigative use.

The policy that was created at the completion of this project adheres to the IACP's and WEF's recommendations and consists of the following sections:

1. *Purpose* - purpose statement defining the role of FRT in police investigations.
2. *Scope* - briefly defines the capabilities and limitations of FRT.
3. *Glossary* - provides commonly used definitions and acronyms.
4. *Procedures* - details procedures to collect and submit a photograph for FRT analysis.
5. *Roles / Responsibilities* - defines roles and responsibilities for the investigator and supervisors during the FRT process.
6. *Authorizations and prohibitions* - specifies when FRT applications are appropriate and defines instances in which FRT will be prohibited.
7. *Reporting / Recordkeeping* - outlines the reporting and recordkeeping process to ensure a record exists of all FRT usage.
8. *Training* - defines the training program investigators and supervisors must undergo to qualify to employ FRT.
9. *Accountability and enforcement* - describes the actions that will be taken for improper misuse of FRT applications.

Lastly, in order to create this policy template, the author borrowed from the standards set forth by the DOJ in a document released in 2017 offering a policy template for law enforcement agencies.

Overview of the Sample

This study was completed using theoretical, purposive, and convenience sampling to gather the documentation required for this project. In this case, documents were chosen based on specific reasons relating to the research question (Ravitch & Carl, 2015). Theoretical and purposive sampling has been applied in researching legal doctrine related to fingerprint and DNA technologies. Theoretical sampling was relevant as only cases that have a high likelihood of replicating future legal challenges that may arise from the introduction of FRT in criminal trials were examined (Ridder, 2017). In purposive sampling, a researcher identifies and selects information-rich cases and contributes to the phenomenon being studied (Etikan, Musa, & Alkassim, 2016). For this research project, the author has only examined court rulings or criminal cases pertaining to fingerprints and DNA that closely aligned with what is believed to be the future legal pathway to FRT being widely accepted into the court system as valid and reliable.

Convenience sampling was employed to identify law enforcement agencies to be utilized in this study. This method involves selecting participants based on practical criteria, such as meeting the requirements of the research project. In this instance, law enforcement agencies that may employ FRT currently, or at some point in the future, were selected (Etikan et al., 2016). To complete this project, the author compiled a list of the forty largest municipal police departments in addition to the ten largest sheriff's offices in the United States as defined by the number of sworn officers. These agencies were used as the sample for collecting and analyzing FRT policies and procedures. All policies have been obtained through open-source methods. The ongoing Covid-19 pandemic has led to a reduction of personnel assigned to Freedom of Information Act (FOIA) requests, leading to a substantial increase in response times or often leading to the request being labeled as "burdensome." Therefore, all information collected was gathered from the publicly available websites of the fifty departments mentioned above.

Additionally, all fifty states in the continental United States and municipalities within these states were examined for existing or pending FRT laws and regulations. These acts and statutes have been examined, analyzed, and discussed, highlighting the limitations of FRT usage that law enforcement agencies have begun to encounter.

Issues of Trustworthiness

Validity is a concept that researchers can employ to ensure their findings are authentic (Ravitch & Carl, 2015). Creswell (2013) summarizes validity as "an attempt to assess the 'accuracy' of the findings as best described by the researcher, the participants, and the readers" (p. 259). In order to validate this research, this author has included the use of theoretical sampling, respondent validation, and transparency through detailing the steps taken for case selection, data collection and the reasons these methods were used (Crowe et al., 2011).

Theoretical validity refers to the ability "to explain the phenomena studied, including its main concepts and the relationships between them" (Ravitch & Carl, 2015, p. 191). While this author did not find extensive research on law enforcement FRT policies, an extensive literature review on facial recognition, similar technologies, the challenges they face to become accepted in legal

proceedings, and legislation governing the use of FRT by law enforcement agencies has been conducted.

Limitations

One of the limits of this paper is that FRT is a novel phenomenon that has only recently seen a large-scale application by law enforcement agencies. This limited timeframe of FRT implementation results in a relatively minuscule amount of available data for examination on the long-term effects of FRT.

A second limitation for this author is the difficulty of being a police officer and separating personal biases to ensuring a fair and balanced approach to this research project. As a police officer, the author embraces the addition of technology that will assist in law enforcement's ability to identify and prosecute criminals. However, as a private citizen, this researcher cherishes Fourth Amendment Rights, along with the right to privacy.

An additional limitation to this paper is the limited data set utilized in reference to police agencies' FRT policies. Only a small percentage of FRT policies will be examined to complete this research project as a significant number of agencies either have not adopted an FRT policy or do not make it available to the public.

Another limitation is the speed at which legislature regarding FRT is being passed into law, which could jeopardize the accuracy of this study. Additionally, as new laws come into existence and departments modify their policies to adhere to these new regulations, the results from this study may become obsolete rather quickly. Lastly, extensive research has not been conducted on law enforcement agencies' use of FRT or the policies that govern this technology.

Results

Comparative Law Review

Understanding the pathways taken to accept fingerprints and DNA evidence in criminal proceedings is paramount to predicting the most likely challenges facing FRT in the coming years. Fingerprints and DNA have not only become admissible in court but are considered crucial pieces of evidence often required to secure a guilty verdict. To accomplish this goal, a brief historical account of landmark cases involving these two technologies follows.

Fingerprint historical account. Fingerprints have been widely accepted as credible and reliable as a means of identification by U.S. courts since the early 1900s. A brief synopsis of several landmark rulings that have arisen since this technology has become a staple in the criminal justice system is presented below.

People v. Jennings (1911): Thomas Jennings was convicted in a criminal court of Cook County (Illinois) on murder charges on February 11th, 1911. Jennings allegedly committed a burglary a short time before and near the vicinity of the murder. Police officers were able to retrieve four fingerprints from a freshly painted porch railing. Subsequently, four witnesses testified in court of their belief that the recovered prints from the railing matched those of Jennings. Jennings appealed his conviction based on a writ of error concerning two questions: the introduction of evidence of other distinct offenses erroneously alleged to have been committed by the plaintiff and the admission of the fingerprints as evidence at trial (*People v. Jennings*, 252 Ill. 534, 1911).

The Illinois Supreme Court affirmed Jennings' conviction with Justice Orrin N. Carter opining "that there is a scientific basis for the system of fingerprint identification, and that the courts are justified in admitting this class of evidence; that this method of identification is in such general and common use that the courts cannot refuse to take judicial notice of it" (*People v. Jennings*, 252 Ill. 534, 1911).

State v. Cerciello (1914): In 1913, Angelo Cerciello was convicted of the murder of his wife. Near the victim's body, police located a bloody hatchet. Police were able to recover fingerprint impressions from the hatchet. Cerciello was placed into custody based on circumstantial evidence. After being in custody for "some time," Cerciello was led by officers into an office and induced to sign his name on a piece of paper. Police officers were able to recover a fingerprint impression from the paper Cerciello signed. The recovered fingerprints were then sent to a fingerprint analyst who testified later in court that the prints recovered from the crime scene were a match from those collected from the paper Cerciello signed.

The court affirmed Cerciello's conviction stating that a defendant's right not to furnish evidence against themselves does not preclude the introduction of the evidence. In this instance, the court agreed that law enforcement officials are within their legal authority to compel a defendant to sign paperwork. The court also concluded that officers are then allowed to collect samples of fingerprints in this manner. Furthermore, those samples may be used for comparison purposes to fingerprints found on crime scenes (*State v. Cerciello*, 86 N.J.L. 309, 90 Atl. 1112, 1914).

United States v. Kelly (1932): Mortimer Kelly was arrested by prohibition agents after allegedly selling undercover agents a pint of gin. Initially, Kelly refused to submit his fingerprints to arresting officers. After being threatened with the idea that his fingerprints would be taken by force if need be, Kelly relented. Upon his release, Kelly requested that his fingerprint records be returned to him (*United States v. Kelly*, 55 F.2d 67, 2d Cir. 1932).

A U.S. District Court ruled that absent a statute, Kelly's constitutional rights had been violated and ordered the return of his fingerprint records. The ruling stated that the procurement of one's fingerprints caused unnecessary indignity to the arrestee. The government appealed, and the case was forwarded to the Second Circuit Court of Appeals, which subsequently reversed the lower court's ruling. Judge Augustus N. Hand opined,

We find no ground in reason or authority for interfering with a method of identifying persons charged with a crime which has now become widely known and frequently practiced both in jurisdictions where there are statutory provisions regulating it and where it has no sanction other than the common law. (*United States v. Kelly*, 55 F.2d 67, 2d Cir. 1932).

Stacy v. State (1930): Vernon Stacy was convicted of burglary in the second degree. Stacy's fingerprints were discovered on the door of a safe located at the scene of the crime. These prints and the fact that Stacy did not have access to the area where the safe was located were the only evidence presented at trial.

The court affirmed Stacy's conviction. The court found that fingerprints are admissible to prove a person's identity and to connect the person with the commission of the offense charged. Additionally, the Honorable PJ Edwards wrote, "The weight and value of the evidence is for the jury...where there is evidence showing that the fingerprints of accused were found in the place where the crime was committed, under such circumstances that they could have been impressed only at the time of the crime, it may be sufficient to sustain a conviction" (*Stacy v. State*, 49 Okl. Crim. 154, 292 P. 885, OK. 1930). Lastly, the court found that during a criminal case, an expert is allowed to demonstrate their knowledge of the subject to the jury through presentations of the pairing of fingerprints of other persons unrelated to that particular case.

DNA historical account. DNA evidence was introduced into the criminal court proceedings in 1986, with the first DNA-based conviction occurring in 1987 (Cormier, et al., 2005). Since then, DNA evidence has been viewed as a valuable tool in proving the innocence or guilt of a person. Below several essential court cases related to DNA evidence are summarized.

State v. Dabney (2003): In 1994, a fifteen-year-old girl was sexually assaulted by an unknown individual. Police were able to recover semen for the offender from the victim's mouth. A DNA profile was created for the then-unknown subject but could not be matched to any DNA profile on record. As the statute of limitations was nearing, prosecutors secured an arrest warrant under the name "John Doe 12." Shortly thereafter, a match was recorded for Bobby Dabney, and the warrant was amended to reflect this revelation. Dabney argued that the arrest warrant did not satisfy the "reasonable certainty," therefore causing the statute of limitations to expire and negating his arrest.

The court affirmed Dabney's conviction with the court ruling that a warrant obtained for a DNA profile suffices the requirement for conferring personal jurisdiction. As the state filed the "John Doe 12" arrest warrant before the expiration of the statute of limitations, it was found that Dabney's due process had not been violated. In their opinion, Justice Wedemeyer found that a DNA profile warrant alone met the requirement for "reasonable certainty" for identification purposes in the obtainment of an arrest warrant (*State v. Dabney*, 2003 WI App 108; 264 Wis. 2d 843; 663 N.W.2d 366, WI. 2003).

District Attorney's Office for the Third Judicial District v. Osborne (2009): William Osborne was sentenced to 26 years in prison following his kidnapping and sexual assault conviction. Years later, Osborne appealed his conviction after being denied the ability to gain access to semen recovered from the scene. Osborne had wanted to send samples of the evidence to a lab of his choosing at his own expense, hoping that technological advances in DNA analysis would prove his innocence.

The appeal was eventually heard by the U.S. Supreme Court in 2009. The Supreme Court ruled against Osborne, finding that advancements in DNA testing technologies should not provide doubt for all past convictions using older methods of testing. The court also ruled that there were already state and federal statutes addressing a defendant's access to evidence post-conviction. In his opinion, Chief Justice Roberts said of the importance of DNA in criminal cases: "DNA testing has an unparalleled ability both to exonerate the wrongly convicted and to identify the guilty. It has the potential to significantly improve both the criminal justice system and police investigative practices" (*District Attorney's Office for the Third Judicial District v. Osborne*, 557 U.S. 52, 129 S. Ct. 2308, 2009, p. 1).

Maryland v. King (2013): In 2009, Alonzo King was booked into Wicomico County jail in Maryland for the charges of first- and second-degree assaults. A buccal swab of King's cheek was conducted and subsequently entered into law enforcement databases during processing into the facility. A short time later, King's DNA profile created from the buccal swab was found to be a match for an unsolved criminal sexual assault that had occurred in 2003. King was eventually tried and convicted for the 2003 rape. However, the Maryland Court of Appeals set aside King's conviction after finding that the collection of DNA samples from felony arrestees violated King's constitutional rights.

In 2013, the United States Supreme Court heard arguments in the case. In a five to four ruling, the court overturned the Maryland Court of Appeals and reinstated King's conviction. The Supreme Court found that after an arrest supported by probable cause, officers are allowed to acquire a DNA sampling from the arrestee. Furthermore, the court ruled that collecting a DNA sample to be a legitimate booking procedure akin to the practices of collecting fingerprints and taking photographs (*Maryland v. King*, 133 S. Ct. 1958, 2013). (See also *Jones v. Murray (1992)* and *Anderson v. Commonwealth (2007)*).

Rules of Admissibility

Summary of the case. Two benchmark rulings encompass the admissibility of scientific-based evidence; the Frye ruling and the Daubert standard. The Frye ruling is derived from a 1923 Court of Appeals decision. In this ruling, the court stated that the evidence must hold general acceptance in the relevant scientific field in which it belongs. Furthermore, the ruling contended that the courts will grant "expert testimony as long as the testimony is deduced from well-recognized scientific principle or discovery" (*Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923)). One of the questions the Frye standard sought to answer is "whether the accepted techniques, when properly performed, generate results accepted as reliable within the scientific community generally" (*People v. Wesley*, 83 N.Y.2d 417, 422, 1994).

Daubert v. Merrell Dow Pharmaceuticals, Inc. (1991), was heard on appeal by the United States Supreme Court in 1993. In their opinion, the United States Supreme Court ruled that a trial judge must assess whether the testimony given by an expert is based upon valid scientific reasoning which can be applied to the facts as they are presented within that particular case. This ruling was adopted from Rule 702 of the Federal Rules of Evidence (FRE), a congressional bill enacted in 1975. Under the Daubert standard (1993), five factors should be considered in determining whether the methodology is valid (*Daubert v. Merrell Dow Pharmaceuticals Inc.*, 509 U.S. 579, 1993):

- Whether the theory/technique in question can be or has been tested.
- Whether the theory/technique has been subjected to peer review and publication.
- Whether the potential error rate of the theory/technique is known.
- The existence and maintenance of standards and controls.
- Whether the theory/technique has widespread acceptance within a relevant scientific community.

Following the *Daubert v. Merrell Dow Pharmaceuticals, Inc.* (1991), the Supreme Court unanimously concurred that Frye no longer applied to the admissibility of scientific evidence post-enactment of the FRE (Moenssens & Meagher, 2014). In 2000, the United States Congress amended the FRE to match the language of the Daubert ruling, thus making Daubert the new standard in Federal Courts when deciding the admissibility of science-based evidence.

Today, thirty-nine states follow the Daubert model, with eight states maintaining the general acceptance theory found under the Frye standard (Moenssens & Meagher, 2014).

Table 1. States Using Frye Rule

California	Illinois	Maryland	Minnesota
New Jersey	New York	Pennsylvania	Washington

The rules of admissibility were adjusted again in 2000 with an amendment to Rule 702 of the FRE following *Kuhmo Tire Co. v. Carmichael* (1999). The court opined that the FRE shall apply to all

expert testimony and not only to scientific based evidentiary evidence (*Kuhmo Tire Co. v. Carmichael*, 526 U.S. 137, 119 S. Ct. 1167, 143 L. Ed. 2d 238, 1999). Today, Rule 702 states (28 U.S.C. 702):

A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:

1. the expert’s scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
2. the testimony is based on sufficient facts or data;
3. the testimony is the product of reliable principles and methods; and
4. the expert has reliably applied the principles and methods to the facts of the case.

Similarities/differences. This section highlights a few of the similarities and differences of court rulings on the admissibility of fingerprint and DNA evidence.

Table 2. Similarities of Fingerprint and DNA in Admissibility Rulings

Similarities
<ul style="list-style-type: none">• Have gained overwhelming acceptance as valid and reliable within their respective scientific fields• As the technologies continue to evolve both are continuously subjected to additional admissibility hearings• Both technologies have been scrutinized under the Frye and Daubert standard

Table 3. Differences of Fingerprint and DNA in Admissibility Rulings

Differences
<ul style="list-style-type: none">• Fingerprints have generally gained acceptance under the Frye standard while DNA has been challenged at a higher rate under the Daubert standard• There is no set standard for a fingerprint examiner to declare a match while DNA follows stringent methods of standards and controls

Evaluation. Fingerprint and DNA evidence have been argued extensively in the matter of these technologies' admissibility. The court's rulings have clearly defined the criteria that must be met for scientific-based evidence to be considered admissible in criminal proceedings. Whether the court jurisdiction is governed by the Frye or Daubert standard is often irrelevant as fingerprints and DNA have gained general acceptance in their respective scientific fields. The most recent admissibility challenges entail disputing novel methods of processing and evaluating evidence.

It was evident during the Daubert ruling that the court considered the regulations set forth by the FRE in their decision regarding admissibility standards. Subsequently, Congress amended the FRE to closely resemble the Supreme Court's opinion found in the Daubert ruling. This altered the landscape of admissibility standards by adopting the Daubert standards in federal court, with

thirty-nine states following suit. Furthermore, following the *Kuhmo Tire* ruling, Congress once again amended the FRE to include expert testimony that was not scientifically-based.

Confrontation Clause / Hearsay Rule

Summary of the case. The Confrontation Clause includes the right of the accused to confront witnesses against them. Two recent court decisions have ruled that some fingerprint evidence is not subjected to the Confrontation Clause. In *State v. Reinhardt*, a South Dakota Supreme Court decision from 2016, it was ruled that fingerprints cards are non-testimonial and therefore not subject to the Confrontation Clause. In a separate case heard in the District of Columbia Court of Appeals in 2021, the court ruled that fingerprints obtained from police records were ultimately non-testimonial and excluded from the Confrontation Clause.

In *State v. Reinhardt* (2016), Troy Reinhardt appealed his conviction for assault with an aggravated sentencing factor as a habitual offender. Reinhardt was convicted of assault. Prosecutors alleged Reinhardt had been convicted of two prior assaults, one in Iowa and another in Nebraska. The prosecution introduced Reinhardt's fingerprint cards from his prior arrests in Iowa and Nebraska to prove that these prior incidents involved Reinhardt. Reinhardt appealed on the notion that his rights had been violated based on the fact he was unable to cross-examine officials from Iowa and Nebraska on the methodology and machinery used to collect the fingerprints. In this ruling, the court stated,

Fingerprint cards are not a solemn declaration or affirmation made for the purpose of establishing or proving some fact. They are physical evidence generated primarily as an administrative step in the booking process as standard practice incident to arrest. Thus, fingerprint cards themselves do not serve a prosecutorial function: absent analysis and testimony, a fingerprint card cannot implicate a defendant. (*State v. Reinhardt*, 875 N.W.2d 25, 2016 S.D. 11, S.D. 2016)

Based on these findings, the court ruled that fingerprint cards do not violate the Confrontation Clause as they are non-testimonial.

In *Grimes v. United States* (2021), Mark Grimes was convicted of possessing a high-powered magazine after police officers recovered a handgun from a vehicle in which Grimes was an occupant. Government forensic specialists were unable to recover fingerprints from the handgun but were successful in retrieving fingerprints from the magazine inside of the firearm. These fingerprints were compared to a fingerprint card obtained from Grimes at the time of an unrelated arrest in 2013. The court ruled that fingerprint cards are not explicitly obtained to "document facts for future prosecution" but rather are an administrative tool used to confirm an arrestee's identity. Therefore, the court found in the State's favor, ruling that fingerprint cards were non-testimonial and not subjected to the Confrontation Clause (*Grimes v. United States*, 252 A.3d 901 (D.C. 2021)).

Similar to fingerprint evidence, DNA has been subjected to numerous challenges based on arguments predicated on the Confrontation Clause. For example, in *Williams v. Illinois* (2012), the U.S. Supreme Court ruled that an expert witness other than the analyst who prepared the report could testify to their opinion of a lab report if it was not entered into evidence. Judge Alito wrote in his opinion,

Modern evidence rules dispense with the need for hypothetical questions and permit an expert to base an opinion on facts made known to the expert at or before the hearing, though such reliance does not constitute admissible evidence of the underlying information" (*Williams v. Illinois*, 567 U.S. 50, 132 S. Ct. 2221, 183 L. Ed. 2d 89, 2012.)

This ruling allows for experts to testify to their interpretation of a lab report's results, even if the expert witness has no knowledge of the methods utilized to obtain the evidence or of the process in which said results were formulated.

In *People v. John* (2016), a New York State of Appeals Court ruled that it had rejected the notion that every analyst involved in the preliminary stages of extraction, quantitation, or amplification was required to be made available to testify at trial. The court stated that any "analyst who witnessed, performed or supervised the generation of defendant's DNA profile, or who used his or her independent analysis on the raw data" would meet the burden set forth in the Confrontation Clause (*People v. John*, 27 N.Y.3d 294, 2016).

In *Washington v. Griffin* (2017), the Second Circuit of the U.S. Court of Appeals agreed that at least one analyst with personal knowledge of the DNA profile workup was sufficient in meeting the Confrontation Clause. More interesting was the recommendation from Judge Debra Ann Livingston that, for "an easier and more efficient route...for cases scheduled for trial, the prosecution could order that a defendant's DNA sample be collected and tested again and supervised by an analyst who is prepared and qualified to testify" (*Washington v. Griffin*, 876 F.3d 395 (2d Cir. 2017)). Judge Livingston continued,

The supervising analyst need not conduct every step of the process herself. Instead, by supervising the process, she could personally attest to the extraction and correct labeling of the sample, that a proper chain of custody was maintained, and that the DNA profile match was in fact a comparison of the defendant's DNA to that of the DNA found on the crime scene evidence. Such testimony would assuage Confrontation Clause concerns, and because the vast majority of criminal defendants plead guilty, only a tiny share of the DNA reports would need to be retested.

The State might retort that such testing and testimony would be unduly expensive, requiring additional time and resources to conduct a DNA test anew and provide a testifying analyst at trial. Those costs, it seems to me, are far outweighed not only by the additional assurance provided by the defendant's opportunity to cross-examine, but also by the exorbitant costs in both time and resources implicated by a defendant's subsequent appeal challenging the denial of such an opportunity. (*Washington v. Griffin*, 876 F.3d 395 (2d Cir. 2017))

Similarities/differences. This section highlights a few of the similarities and differences of court rulings on fingerprint and DNA evidence in reference to the Confrontation Clause and the Hearsay Rule.

Table 4. Similarities of Fingerprint and DNA Confrontation Clause / Hearsay Rulings

Similarities
<ul style="list-style-type: none">• Not all participants in the process of obtaining the evidence are required to be made available to testify in court proceedings.• Evidence obtained through normal booking procedures are not considered hearsay evidence and not subject to the Confrontation Clause.

Table 5. Differences of Fingerprint and DNA Confrontation Clause / Hearsay Rulings

Differences
<ul style="list-style-type: none">• DNA expert witnesses must have witnesses, supervised, or performed the testing process or utilized the raw data to come to their conclusions, whereas fingerprint evidence is not subjected to these standards.• DNA evidence is rapidly evolving in comparison to fingerprints and has received more scrutiny as of late as to the methods and standards of testing and processing.

Evaluation. The courts have ruled that regular booking procedures such as photographing and fingerprints are not considered hearsay evidence and not subject to the Confrontation Clause as they are not taken for explicit use in future criminal trials. While DNA collection is not necessarily a part of the routine booking process, the courts have allowed for states to mandate the collection from those persons convicted of certain felonies. This also allows for DNA collected through these methods to pass muster in Confrontation Clause legal challenges. Recent court rulings have also allowed the prosecution to refrain from the arduous task of subpoenaing every individual involved in testing and analyzing scientific evidence.

Several court rulings have made direct reference to individual state and federal laws pertaining to the collection of fingerprint and DNA samples from arrestees or prisoners in their rulings of Confrontation Clause challenges. For example, since 2005, the federal government has required all persons arrested for a federal crime to provide a DNA sample (Bernson, 2009), and all 50 states in the U.S. have laws regulating offenders convicted of certain crimes provide DNA samples which are then entered into law enforcement databases (Bernson, 2009). These laws have shaped court rulings to allow a significant amount of DNA evidence to be accepted, as these samples are not directly gathered for the purposes of future criminal proceedings.

Fourth Amendment

Summary of the case. The Fourth Amendment of the United States Constitution protects citizens from unlawful search and seizures absent a warrant. For decades law enforcement officials have collected fingerprints from arrestees and stored them in local and federal catalogs. More recently, some arrestees are being forced to provide blood or saliva samples to create a DNA profile that will be entered and stored into government databases. Each is collected for a multitude of purposes, including identification at the time of arrest, but is also employed as a means to identify perpetrators in future crimes. The latter has been subject to numerous court challenges regarding the legalities of storing this type of information.

Since 1924, the FBI has amassed and collected fingerprint cards from law enforcement agencies (Moses, 2014); this system has evolved into the Automated Fingerprint Identification System, storing tens of millions of fingerprint records (Moses, 2014). In 1994, Congress authorized the Combined DNA Index System (CODIS), connecting DNA laboratories at the local, state, and national levels (FBI, 2019). Run by the FBI, the index has amassed millions of DNA profiles (FBI, 2019).

Long-standing court rulings have classified fingerprint collection at the time of an arrest to be a legal process used in the identification of the arrestee. Two court cases highlight this sentiment. In *Smith v. United States* (1966), the court ruled that "it is elementary that a person in lawful custody may be required to submit to photographing" (*Smith v. United States*, 324 F.2d 879, 882, D.C. Cir. 1963). In *Napolitano v. United States* (1965), the court opined that the "taking of fingerprints in such circumstances is universally standard procedure, and no violation of constitutional rights" has occurred (*Napolitano v. United States*, 340 F.2d 313, 314, 1st Cir. '65). The U.S. Supreme Court clarified that the fingerprint evidence must have been obtained in a legal manner, and detaining someone for the sole purpose of obtaining one's fingerprints is a violation of the Fourth Amendment and inadmissible in criminal proceedings (*Davis v. Mississippi*, 394 U.S. 721, 1969). The notion that databases of fingerprints collected from arrestees were constitutional and not in violation of the Fourth Amendment was affirmed in court rulings on DNA evidence. These cases are presented below.

One landmark ruling, *Jones v. Murray* (1992), set the legal precedent for the constitutionality of DNA databases along with tacit approval for similar technologies such as fingerprint databases. In 1990, six inmates of the Virginia correctional institution filed suit against a Virginia law requiring convicted felons to submit blood samples for DNA analysis to determine identification characteristics and the creation of a data bank that would allow access of the information to law enforcement officers. The inmates argued that the collection and storage of blood samples violated their Fourth Amendment rights.

Virginia successfully convinced the court that collecting blood samples was acceptable under the "special needs" exception to the Fourth Amendment due to a need to identify persons in custody. The court concurred, stating that a state has a legitimate interest in identifying those persons in their custody arrested with probable cause (*Jones v. Murray*, 962 F.2d 302, 4th Cir. 1992). The court went further in their opinion (1992):

When a suspect is arrested upon probable cause, his identification becomes a matter of legitimate state interest, and he can hardly claim privacy in it... identification of suspects is relevant not only to solving the crime for which the suspect is arrested, but also for maintaining a permanent record to solve other past and future crimes. This becomes readily apparent when we consider the universal approbation of "booking" procedures that are followed for every suspect arrested for a felony, whether or not the proof of a particular suspect's crime will involve the use of fingerprint identification...therefore, we find that the Fourth Amendment does not require an additional finding of individualized suspicion before blood can be taken from incarcerated felons for the purpose of identifying them.

In 2013, the United States Supreme Court ruled on *Maryland v. King*. In a split decision, the court ruled again that the collection of DNA at the time of arrest was a routine part of the booking process and a valuable tool for law enforcement in identifying arrestees. This case is important

because the DNA sample was collected at the time of arrest and submitted to CODIS prior to conviction. The majority opinion was that the need for law enforcement to identify an arrestee due to safety issues, not only for law enforcement officers but the general public, outweighed the need for privacy for the arrestee (*Maryland v. King*, 569 U.S. 435, 133 S. Ct. 1958, 186 L. Ed. 2d 1, 24 Fla. L. Weekly Supp. 234, 2013).

Similarities/differences. The collection and storage of fingerprints and DNA samples have followed a similar path regarding their acceptance under the Fourth Amendment. The differences are minuscule enough to make them not relevant for discussion. Highlighted here are some of the important similarities found throughout the above cases:

Table 6. Similarities of Fingerprint and DNA in Fourth Amendment Rulings

Similarities
<ul style="list-style-type: none">• Fingerprint and DNA collection are accepted as a normal part of the booking process for an arrestee.• The collection and storage of these biometric identifiers have been found not to violate the Fourth Amendment.• Both are understood to be useful tools in the identification of arrestees.

Evaluation. The processes of fingerprinting and recovering samples for DNA analysis have been deemed lawful, a normal part of the booking procedure, and minimally intrusive. Under the "special needs" provision, the collection of this data is said to be used for identification purposes. In *Jones v. Murray*, the court ruling stated that the storage of said data holds a legitimate state interest in not only identifying the person under arrest at that particular moment but also in solving past and future crimes. The rulings allow for law enforcement agencies to collect and store a plethora of biometric data that could be used for future criminal proceedings. In *Maryland v. King*, Justice Scalia dissented from the majority. He believed that placing DNA sample collection under the umbrella of identification of an arrestee was improper. Scalia wrote that the average return time for DNA evidence was "months." In contrast, the average fingerprint was returned from the Automated Fingerprint Identification System (a system managed by the FBI that all law enforcement agencies submit arrestee fingerprints to) in 27 minutes.

Fingerprint and DNA collection and storage have been found in compliance with the Fourth Amendment as long as these samples were collected in a lawful manner. Virginia was the first state to mandate convicted felons of certain offenses to submit DNA samples for inclusion in a DNA databank. Following the *Jones v. Murray* decision, many other states followed suit with the federal government enacting federal laws in 2005, forcing those convicted of federal felonies to submit DNA samples. These laws have allowed the federal government to collect tens of millions of pieces of biometric data on citizens, often used later for other criminal investigations not related to the original offense. To date, fingerprints are collected from every arrestee in custody of a law enforcement agency. DNA collection laws vary by state, with most abiding by the rule that a person must have been convicted of a felony offense, although some jurisdictions allow collection upon a felony arrest.

Review of Policies

The policy data was collected by examining the 40 largest municipal police departments and 10 largest county Sheriff's Departments in the United States. The below chart presents these agencies along with the number of sworn personnel belonging to each department (Kershner, 2020; Top 10, 2020).

Table 7. Largest Police Departments in the U.S.

Police Department	Number of Sworn Officers
New York Police Dept. (NY)	36,008
Los Angeles County Sheriff (CA)	18,000
Chicago Police Dept. (IL)	11,965
Los Angeles Police Dept. (CA)	9,870
Cook County Sheriff (IL)	7,000
Philadelphia Police Dept. (PA)	6,031
Broward County Sheriff (FL)	5,500
Houston Police Dept. (TX)	5,203
Washington Metropolitan Police (DC)	3,712
Harris County Sheriff (TX)	3,500
Dallas Police Dept. (TX)	3,408
Miami-Dade Police Dept. (FL)	2,723
Phoenix Police Dept. (AZ)	2,689
Las Vegas Metropolitan Police (NV)	2,566
Baltimore Police Dept. (MD)	2,524
Hillsborough County Sheriff (FL)	2,500
Nassau County Police Dept. (NY)	2,462
Suffolk County Police Dept. (NY)	2,385
San Francisco Police Dept. (CA)	2,356
Detroit Police Dept. (MI)	2,250
San Antonio Police Dept. (TX)	2,244
Orange County Sheriff (CA)	2,100
Boston Police Dept. (MA)	2,099
Memphis Police Dept. (TN)	2,012
Honolulu Police Dept. (HI)	1,962
Milwaukee Police Dept. (WI)	1,879
Baltimore County Police Dept. (MD)	1,869
San Diego Police Dept. (CA)	1,857
Columbus Police Dept. (OH)	1,838
Austin Police Dept. (TX)	1,807
Charlotte-Mecklenburg Police Dept. (NC)	1,743

Atlanta Police Dept. (GA)	1,730
Prince George's County Police Dept. (MD)	1,650
Jacksonville County Sheriff (FL)	1,650
Sacramento County Sheriff (CA)	1,600
Fort Worth Police Dept. (TX)	1,541
San Bernardino County Sheriff (CA)	1,540
Riverside County Sheriff (CA)	1,500
Cleveland Police Dept. (OH)	1,475
Denver Police Dept. (CO)	1,464
Metropolitan Nashville Police Dept. (TN)	1,403
Seattle Police Dept. (WA)	1,373
Fairfax County Police Dept. (VA)	1,369
Kansas City Police Dept. (MO)	1,364
Louisville Metropolitan Police Dept. (KY)	1,246
Montgomery County Police Dept. (MD)	1,230
St. Louis Police Dept. (MO)	1,175
Oklahoma City Police Dept. (OK)	1,101
Cincinnati Police Dept. (OH)	1,032
El Paso Police Dept. (TX)	1,026

Using open-source data collection methods, this researcher attempted to locate if each agency made available to the public their FRT policy or directive. The researcher also attempted to verify if the agency acknowledged or denied the use of FRT programs.

This inquiry led to the collection of seven FRT policies. These policies range in length from one to eight pages. The median length was just under four pages. The three most recently published policies have effective dates in 2020. The oldest policy was published in 2013. The table on the following page illustrates the police departments in which policies were found and examined, along with the total number of pages in the policy and the year they were made effective.

Table 8. Police Policies

Police Department	Total Pages	Year Published
Atlanta P.D (GA)	3	2020
Baltimore County P.D. (MD)	2	2017
Chicago P.D. (IL)	1	2013
Detroit P.D. (MI)	8	2019
Honolulu P.D. (HI)	4	2015
Miami P.D. (FL)	4	2020

New York City P.D. (NY)	4	2020
-------------------------	---	------

The remaining 43 police departments either did not use FRT, or do not have a publicly viewable copy of their policy. Nineteen departments appear to utilize FRT, but no policy could be located. Eleven departments claim they do not use FRT at this time, while two departments previously used FRT but due to legislation have suspended those programs. Ten police agencies have not acknowledged whether FRT is available to their members, and no policy could be found at this time. Riverside Police Department, located in California, has a publicly viewable policy, but this policy was created by the FRT application vendor and was not specific to Riverside P.D.; thus, it was not used for the purposes of this study.

Below is a list of the essential elements for individual FRT policies, followed by Table 9, which indicates whether or not each individual policy incorporates the recommended elements.

- *Describes the process of FRT*- Describes the process for collecting/submitting images for comparison, the process for evaluating returned images, and related information applicable to the use of FRT.
- *Limits the scope of utilization* - Describes the actions that would allow or prohibit a member from utilizing FRT.
- *Oversight process* - Details procedures in which supervisors monitor FRT programs to ensure accuracy and compliance with existing laws and policies.
- *Training program* - Describes a training regimen that FRT operators and requesters undergo prior to FRT usage.
- *Verification mechanisms* - Describes in the process in which returned images can be considered a match or the manner in which a match photograph will be considered viable.
- *Record keeping standards* - Defines the process in which FRT usage records to include requests, submissions, and returned images are stored and the process in which those records would be made available to the public.

Table 9. Evaluation of Police Department Policies

Police Department	Describes Process	Limits Scope	Oversight Process	Training Program	Verification Mechanisms	Record Keeping
<i>Atlanta P.D.</i>	Yes	Yes	Yes	Yes	No	Yes
<i>Baltimore County P.D.</i>	No	Yes	No	No	No	No
<i>Chicago P.D.</i>	No	No	No	No	No	No
<i>Detroit P.D.</i>	Yes	Yes	Yes	No	Yes	Yes
<i>Honolulu P.D.</i>	Yes	No	No	No	Yes	No
<i>Miami P.D.</i>	Yes	Yes	No	No	Yes	Yes
<i>New York P.D.</i>	Yes	Yes	Yes	No	Yes	No

Describes the process of FRT. Five out of the seven departments examined describe procedures pertaining to the collection, submission, and examination of photographs submitted for FRT analysis. Some policies define a thorough process while others give a short summarization of the process. Depicted below is a brief overview of each of the five department's policies regarding this process.

Table 10. Describes the Process of FRT

<i>Atlanta P.D.</i>	Members will submit photographs to the appropriate FRT unit which will then conduct a search and return the results to the requesting investigator.
<i>Detroit P.D.</i>	Members will submit probe photograph to unit that conducts FRT. This unit will perform search. If viable candidates are returned from said search, results will be returned to requestor.
<i>Honolulu P.D.</i>	Members will submit a photograph to unit that conducts FRT. Analysis will be done using Honolulu's intradepartmental database. If no results are located a request to send photograph to FBI for analysis can be made.
<i>Miami P.D.</i>	Members will submit a photograph to the FRT unit who will then conduct a search of the program and provide all search results and pertinent information to the requestor.
<i>New York P.D.</i>	Member will locate and submit photograph. Photo will be analyzed for possible matches. Report will be generated and sent back to investigator.

None of the policies specifically describes how the search is conducted or the manner in which the results are calculated. Each department has a unit within the department that conducts its facial recognition program or outsources to a third-party vendor. All policies, in essence, state for the requestor to submit the photograph to said unit, which will then conduct the analysis and return the results to the investigator.

Limits the scope of utilization. A policy was found to limit the scope of FRT if the policy specified restrictions on the use of this technology. Chicago and Honolulu Police Departments were the only two agencies with available policies that failed to advise members of any restrictions on when a member could submit a photograph for analysis. The following table highlights the remaining five departments and brief summaries of the restrictions given to their members.

Table 11. Specifies the Restrictions of the Utilization of FRT

<i>Atlanta P.D.</i>	Only use photographs for analysis found in the public domain.
<i>Baltimore County P.D.</i>	States the member must have a valid "work related" purpose.
<i>Detroit P.D.</i>	Members may not utilize FRT solely based on a person's: religious, social, political views; participation in a lawful event; race, ethnicity, gender, disabilities, or sexual orientation.
<i>Miami P.D.</i>	Ensures that all FRT uses are consistent with authorized purposes while not violating the privacy, civil rights, and civil liberties of individuals.
<i>New York P.D.</i>	FRT may only be used to identify a possible criminal, missing person, crime victim, deceased person, person unable to identify themselves, a person in custody who otherwise cannot be identified, or to mitigate an imminent threat.

The Detroit Police Department was the only agency to mention the First or Fourth Amendments to the U.S. Constitution. Baltimore County P.D. states only that a member will have a valid "work related" purpose but does not define the meaning of "work related" and does not place any restrictions on this term. New York P.D. produces the most extensive list out of the seven policies, in which employees may submit photographs into FRT programs. Lastly, Atlanta P.D. restricts members to photographs that are located in the public domain. The policy does not seem to allow for photographs in possession of the Atlanta officers, such as booking photographs. The only policy that contains language that prohibits FRT in real-time applications is the Detroit Police Department.

Oversight process. Only three of the seven policies mention supervisory responsibility in the FRT process. The remaining four either have no requirements for supervisor intervention or fail to specify the stages of this process that require supervisor participation or approval.

Table 12. Specifies the Oversight Process of FRT

<i>Atlanta P.D.</i>	Employs multiple levels of review. The employee's immediate supervisor will review the request before forwarding to the commanding officer of the unit overseeing the FRT program.
<i>Detroit P.D.</i>	A supervisor is part of the submission process but also is required to sign off on any matching return image candidates.
<i>New York P.D.</i>	Requires review from immediate supervisor prior to submission of probe photograph. FRT unit supervisor must review any and all matches before a return to requesting investigator.

New York and Detroit Police Departments employ multiple levels of supervisory oversight. This process includes supervisor participation at the pre and post levels. Atlanta P.D. requires two supervisors to sign off on the FRT request but does not include supervisor input beyond the initial

stages. The other departments do not explain what, if any, roles a supervisor plays in these FRT programs.

Training program. Only one policy defines any training requirements to participate in FRT programs. Atlanta P.D. requires its employees (sworn and civilian) to attain training equivalent to that of an investigator. Furthermore, personnel are mandated to have been trained in intelligence gathering and/or cyber investigation training. To attain the role of FRT administrator, the employee must have completed all training required by the authorized vendor of the FRT program.

No other policies could be found that mention training that an investigator is mandated to complete before selecting or submitting probe photographs. Furthermore, no training mandates could be located within these policies that define that knowledge or experience for those who are conducting the FRT or selecting matching photographs before returning them to the submitting officer.

Verification mechanisms. Four of the seven policies examined detail the process in which a match photograph is verified. While none of the polices describes the method in which a photograph would be considered a match, the following four policies have a process in which multiple persons must confer and agree on the validity of a possible match.

Table 13. Specifies the Verification Mechanisms of FRT

<i>Detroit P.D.</i>	Matches must be peer reviewed and corroborated by at least one additional examiner before being returned to the requesting officer.
<i>Honolulu P.D.</i>	The FRT examiner will determine if a match is located, which will then be sent back to requestor with an analysis of how the examiner came to their conclusion and the steps that were taken during this process.
<i>Miami P.D.</i>	Results will be corroborated between the examiner and requestor.
<i>New York P.D.</i>	Any possible matches must be peer reviewed before return to requesting investigator, who is then required to conduct further investigation to determine if said match is connected to investigation.

All four polices above convey that a match photograph is to only be considered as an investigative lead. The requestor is responsible for conducting a follow-up investigation to determine if the match photograph relates to a person connected to the crime in question. New York P.D. and Detroit P.D. are the only departments that require a peer review of the FRT results before they are sent back to the initial requestor. Miami P.D. briefly mentions that the examiner and requestor must corroborate results, while Honolulu P.D. only requires that the examiner include a report describing the process that led to their conclusion.

Record keeping standards. A department was given a "yes" in this category if the author could locate mention of storing requests/results from the FRT program. After examination it was determined that three of the seven departments studied adhere to any method of record keeping.

Table 14. Details the Record Keeping Practices

Atlanta P.D.	A log of all investigations requiring FRT assistance shall be maintained and reviewed on a quarterly and annual basis.
Detroit P.D.	Will maintain records of FRT requests and returns for a minimum of one year. This information will include requesting officer's information, case file number, and date of request.
Miami P.D.	The requesting investigator will maintain all search results in investigative file. Requires monthly audits by supervisors.

The three policies above require the retention of FRT usage, but only Detroit P.D. includes a definitive timeframe in which these records are required to be maintained. All record keeping revolves around the ability of the department to conduct audits at various intervals. No policy makes mention of record keeping for the purposes of transparency or the availability to produce records for requests for information, such as Freedom of Information Requests.

Discussion

This report highlights the increasing utilization of FRT programs, particularly those used in law enforcement agencies. A plethora of obstacles await this technology as it becomes more mainstream in criminal investigations. By comparing the pathways of existing technologies (fingerprints and DNA evidence) into general acceptance in courtroom settings, this author will suggest recommendations for law enforcement agencies to implement their own FRT programs. Borrowing from current best practices at the federal, state, and local levels, this author will present a generic template that can be modified to assist a law enforcement agency with creating an FRT policy going forward. A department that effectuates a stringent set of rules and regulations complemented with a well-rounded FRT policy will allow their agency to conduct more thorough criminal investigations, to be better prepared for future court challenges, and to remain at the forefront of training as this technology evolves.

Law Review

Laws and regulations. The literature presented a number of states and municipalities that have rushed to implement restrictions on FRT usage by law enforcement agencies. It appears, in this author's opinion, that a number of these restrictions were enacted in a knee-jerk fashion based solely on uniformed public opinion. When used in a lawful manner, FRT programs can assist law enforcement in numerous ways and not only in circumstances that would lead to a criminal prosecution. Outright bans on the application of this technology solely for law enforcement agencies seem arbitrary considering that facial recognition is already a mainstay in other governmental programs (e.g., REAL ID) and private sector applications (e.g., cellphone manufacturers and social media platforms). A more equitable approach would be to gather all relevant stakeholders and map out a solution that would protect the constitutional rights of the citizens while allowing law enforcement officers to capitalize on a revolutionizing piece of technology.

Legal challenges. The pathways undertaken by fingerprint and DNA evidence lead this author to believe that FRT will succeed in gaining acceptance as reliable evidence with a caveat; this evidence will need to be verified by humans before further action is taken during the course of an investigation. As found in *People v. Reyes* (2020), police officers did not solely rely on the returned match of Luis Reyes. Once a return was made from the FRT program, officers utilized countless other booking photographs and were able to match tattoos taken from the surveillance photographs, leading officers to have enough probable cause to make an arrest in the case. This author believes that similar methods of verification will be successful in challenges invoking confrontation clause issues.

The rules of admissibility. While the waters have yet to be tested concerning the admissibility of FRT, this author believes that this technology will be successful. Under optimal conditions, such as those standards set forth by the FBI's NGI program, it can be argued that FRT meets the majority of requirements found in the five factors of the Daubert standard.

1. *Whether the theory/technique in question can be/has been tested.* The FBI's algorithms and processes are subjected to an annual review by the National Institute of Standards and

Technology. While there are 127 commonly used algorithms currently in use, each can be independently tested.

2. *Whether the theory/technique has been subjected to peer review and publication.* FRT has been subjected to numerous peer review studies and subsequently published.
3. *Whether the potential error rate of the theory/technique is known.* As of 2018, the FBI boasts algorithm software that claims a 99.12% Rank 1 accuracy, meaning that the first photo the algorithm produced was a correct match over 99% of the time.
4. *The existence and maintenance of standards and controls.* The FBI employs a stringent set of standards for their FRT program which can be located in their "Federal Law Enforcement use of Facial Recognition Policy." As a result, law enforcement agencies that outsource their FRT to third-party vendors will likely face harsher scrutiny.
5. *Whether the theory/technique has widespread acceptance within a relevant scientific community.* FRT and other machine learning applications have generally gained acceptance within the scientific community, but this author believes there will be significant numbers of experts inclined to testify for or against this technology at admissibility hearings.

Again, the above scenario assumes that a law enforcement agency utilizes the FBI's FRT database and programs. A sizeable portion of law enforcement agencies contract out to third-party vendors to complete FRT requests, while some perform these functions in-house by comparing previously obtained booking photos. As this technology evolves into criminal proceedings, it will require multiple admissibility challenges to each vendor or program—and possibly to each algorithm. This will prove costly and time-consuming, but it is necessary to vet these methods and techniques to assess their reliability and acceptance in the scientific field and a court of law.

Additionally, the Federal Rules of Evidence govern that judges must assess whether testimony given by an expert is based upon valid scientific reasoning and can be applied to the facts presented within a particular case. With respect to FRT, expert testimony should be found to be admissible as a well-recognized scientific principle or discovery, seeing that this technology is rapidly gaining acceptance in the scientific field. To accomplish this objective, it will become imperative for the agency to employ and/or train specific employees with extensive knowledge of the program authorized for use by the organization.

Confrontation Clause / Hearsay Ruling. The Supreme Court has ruled that booking photos and fingerprints obtained at the time of arrest are legal, not intrusive, and part of routine arrest procedures used to confirm an arrestee's identity. Therefore, FRT return matches generated through a database exclusively containing booking photographs are highly likely to be considered non-testimonial, resulting in exclusion from the Confrontation Clause. A significant point of contention will more than likely arise from returns where the return image was hosted by a third-party vendor or where the comparison image was scraped from the internet.

Fingerprint and DNA technology have not been subjected to third-party involvement, to the best of this author's knowledge. These parcels of evidence are usually collected at the crime scene and later submitted to laboratories for analysis. Post-analysis, these samples are compared to specimens that have been collected through other criminal justice means, such as prior arrest or condition of parole, to name two examples. The exception to this process has been the novel introduction of genetic genealogy. In these instances, officers submit DNA evidence collected to third-party vendors (23andMe, Ancestry, GEDmatch) in the hopes of receiving a match or an investigative lead from a distant relative that may point to an individual of interest.

These cases are rare to date and have not faced extensive legal scrutiny as to the manner in which the samples were compared. However, in 2019, a Florida judge granted police access to the entire database of GEDmatch for the purpose of suspect identification (Kaiser, 2019). Legal scholars are at odds over the legalities of this process and argue a host of issues, including consent of the genealogy database customers, the victim, and the suspect.

The second aspect of the Confrontation Clause / Hearsay ruling revolves around expert testimony. The courts have ruled that the state needs only to provide an analyst who witnessed, performed, or supervised the comparison or who used an independent analysis of the raw data. Law enforcement agencies that submitted the photograph could meet this burden as long as this individual was trained and certified in FRT protocol. This issue could be addressed in the department's training section within their individual FRT policy.

Fourth Amendment. Much like the Confrontation Clause, collecting photographs during routine booking procedures have passed scrutiny in meeting the standards of the Fourth Amendment. This author cannot imagine that comparison photographs from a cache of booking images would be any different. Law enforcement agencies have access to millions of these images courtesy of the FBI. Following previous court rulings regarding the collection and retention of fingerprints, it can be assumed that limited legal challenges will arise when FRT is performed within the law enforcement community.

Again, like the Confrontation Clause, it appears as if the more significant legal battles will be waged in instances in which comparison images are collected through third-party means. The first issue that may arise is the manner in which law enforcement gained access to the target image, such as surveillance video or still photographs. This subject has already been argued and affirmed in court as admissible and covered under the Federal Rules of Evidence (Larmon, 2021). As mentioned earlier in *People v. Reyes* (2020), the court's opinion of officers viewing the surveillance video was admissible as the officers were viewing the video for the purpose of identifying the individual committing the unlawful act. The above facts suggest that usage of FRT from these images, through the collection of these types of evidence, will be affirmed by the courts as lawful.

The outcome becomes murkier when target or probe images are collected on the public way. The courts have ruled that, much like vehicles, a person loses most of the privacy protections offered under the Fourth Amendment once on the public way. In *United States v. Knotts* (1983) and *Olmstead v. United States* (1928), the courts have stated that a person in a public place has no right to privacy as their movements can be observed by any member of the public with the naked eye and that visual surveillance does not constitute a search. A plethora of arguments could be

presented for allowing or opposing these images into court proceedings, especially if the probe photo was not taken during the commission of a crime.

Lastly, and what this author believes will become the biggest challenge for admissibility under the Fourth Amendment, are comparison images that have been collected and stored from third-party vendors and those scraped from open-source intelligence methods. *Jones v. United States* (2012) stated that persons do not have an expectation of privacy relating to data volunteered to third-party companies as long as that data is maintained over the course of normal business. How this relates to persons posting pictures of themselves on Facebook, which then end up being used as comparison images in private companies' FRT detection programs, has yet to be determined by the courts.

In this author's opinion, the majority of these complications can be accounted for with a strong policy and procedure. If a police entity limits itself to utilizing photographs collected and stored through normal law enforcement operations, the rate of successfully introducing this novel technology into criminal proceedings will be significantly higher than in instances where third-party vendors participate.

Policy Discussion

The fact that only seven policies could be located for the nation's largest 50 municipal and sheriff agencies is troublesome, to say the least. Two possibilities exist from this revelation; only 14% of large law enforcement agencies are currently utilizing a novel technology that may assist in solving and preventing violent crimes, or a large percentage of agencies are employing this technology but failing to notify the general public of its use. In an era of transparency, there are few instances in which police department policies are not made available to the constituents they serve.

Upon final examination of the above policies, this author feels each of the seven examples are deficient in multiple categories. The Chicago Police Department's meager one-page document created more than nine years ago emerged as the most deficient as it failed to address any of the variables inspected. The general order serves no purpose other than stating that the Bureau of Detectives is responsible for the FRT procedures; it fails to state what the procedures are. The Atlanta and Detroit Police Departments offered the most comprehensive examples obtained for this study, but this author feels even these policies should undergo extensive revisions to maximize their effectiveness going forward.

Describes the process of FRT. While the majority of policies discussed this variable, all were brief and failed to explain key elements of this process. An effective policy should explain in detail the following steps of the FRT process:

1. *Authorized personnel.* At minimum, this section of the policy should designate which personnel are authorized to request FRT, and the training programs in which they must have completed prior to this request. There should be no need to describe in detail the actual training programs as this will be covered in a separate section of the policy.

2. *Methods for obtainment and selection of a target photograph.* This section should explain to investigators the various sources where a target photograph may be located. Investigators should be made aware of the qualities of photos that will be most likely to yield a match. These characteristics might include lighting, view of target's face (preferably a picture where target is facing the camera), size, and pixelation.
3. *Process for submitting the photograph.* A policy should describe the process for photo submission. This shall include the forms/paperwork necessary to begin the FRT process, the personnel that will review said paperwork and ensuring the quality of the photograph submitted meets the minimum standards, and if the FRT program is conducted by members within the agency or outsourced to a third-party vendor.
4. *Verification process.* In the same regard as the description of the training program, this step in the process can be brief. This section will also be covered in greater detail in a separate section, but should briefly describe the process in which a photograph is deemed a match, the minimum similarity scores for target images, and the number of target photos returned.
5. *Next steps.* This section of the policy shall include next steps in the investigative process that investigators should adhere to in continuance of their investigation. The return images shall be documented in a report and inventoried for future court proceedings. In addition, investigators should be reminded that returned photographs are not conclusive; they should only be used as investigative tools in identifying suspects and are not to be used as probable cause to effect an arrest. Furthermore, a process should be identified for instances in which probe images fail to identify possible match candidates.

None of the policies examined explained the methods of obtaining a target photograph. There are many ways for an investigator to obtain a target photo, such as surveillance video, a suspect's social media accounts, or an image recovered from a victim or witness's cellular device. Furthermore, no policies described the minimum requirements that an image must possess to be considered viable for inclusion in the FRT process.

The policies utilized for this study that included a section describing the process were generic and highly vague. All of the examples simply required the photographs to be submitted to the unit for analysis. No policy described the method or algorithm that would be used for analysis, nor detailed the process in which a similarity score would be applied to determine target photographs returned to the investigator.

Similarly, these policies failed to describe the next steps taken in an investigation. While it is this author's belief that this section should be made relatively generic and not all-encompassing in accordance with individual agencies' investigative procedures, the lack of this specific element is glaring. At minimum, the process for documenting and preserving the evidence should be specified. Failure to maintain a proper chain of custody may have negative implications in future court proceedings.

Limits the scope of utilization. An integral undertaking in an FRT process is the delineation of prohibitions and authorizations of the FRT program. Atlanta and Baltimore County's description of prohibitions is too generic to be effective. For example, Atlanta P.D. states that only photographs "found in the public domain" must be submitted for analysis. Atlanta defines the public domain as:

The state of belonging or being available to the public as a whole, and therefore not subject to copyright. The term "public domain" refers to creative materials that are not protected by intellectual property laws such as copyright, trademark, or patent laws. The public owns these works, not an individual author or artist. Anyone can use a public domain work without obtaining permission, but no one can ever own it.

Many questions arise from this definition. Images captured from private surveillance video are, in essence, owned by the individual that possesses the surveillance camera network. Does this disallow images recovered from these types of networks to be submitted for analysis? Are images that are captured from city-owned camera systems authorized? What about images collected from open-source intelligence avenues such as images scraped from the internet? Definitions such as these become too speculative to serve a useful purpose.

Detroit, Miami, and New York Police Departments were the only departments to mention the First or Fourth Amendments to the Constitution. To instill public trust into a department's FRT policy, the inclusion of this language is imperative. The public and members of the particular agency should be made fully aware that FRT will not be made available for use on members of the public exercising their rights protected under the U.S. Constitution. New York P.D. goes further and explicitly describes the limited instances in which FRT programs may be made available.

Oversight process. Equally crucial to limiting the scope of authorization is a clearly defined oversight process. The Atlanta Police Department was the only agency in this study that included multiple levels of review. The immediate supervisor of the investigator requesting the use of the FRT program and the commanding officer of the FRT program are required to sign off prior to utilization of an FRT application. The majority of agencies in this study make no mention of an oversight process or describe the responsibilities of departmental supervisors. Detroit and New York P.D. require a supervisor to participate during the submission process and post-return of image candidates, but they do not specify if a single supervisor suffices or if multiple supervisors should be involved throughout the procedure.

A clear explanation for each supervisory role within the program needs to be given. Stating that a supervisor simply reviews the submission is too ambiguous and will lead to a failure of supervision. A supervisor should have the ability to refer to a document and know with absolute certainty what their role in the process is. None of these policies offered such elucidation of this process.

Additionally, part of the oversight process should outline disciplinary procedures for misuse or abuse of the FRT program. Including the terms of discipline will again lead to higher acceptance rates amongst the public. Discipline was mentioned zero times in any of the seven policies studied for this project.

Verification mechanisms. Verification procedures may well be the most critical step in the FRT process. A policy that describes the in-depth course of actions that will lead to an analyst declaring a high probability match will become imperative to this technology gaining acceptance as reliable evidence inside a courtroom. None of the department policies described the process that resulted in possible matches being returned to the submitting investigator. The lack of a defined set of standards and procedures will render FRT ripe for legal challenges should it become a tool incorporated in a criminal investigation.

New York and Detroit P.D. require that matches are peer-reviewed before being returned to an investigator but again fail to describe what is involved in this process. Honolulu P.D. requires that the examiner complete a report that will be sent to the requestor describing the steps taken during the process and how the analyst came to their conclusion. This, in the author's opinion, is the strongest example of demonstrating verification mechanisms, although this policy still falls short in that there is no peer review specified in the process.

Record keeping. Only three of the policies make mention of any record keeping. As this technology has already received negative press and is not well understood by the general public, record keeping will have the most considerable impact on transparency. This aspect is severely lacking, similar to the previous elements discussed in the seven policies. Four of the seven agencies do not mention any process for storing and/or maintaining FRT requests or usage. Detroit P.D. states that records will be stored for a minimum of one year but again does not mention the types of information collected or the purpose of its collection. Atlanta P.D. conducts quarterly and yearly audits of their FRT program, while Miami P.D. requires monthly audits to be completed by supervisors; neither policy specifies what information will be collected or the auditing process.

This author would suggest that, at minimum, a policy detail the exact information to be collected. This should include the requestor's information, case file number, copy of probe photograph, copy of all records pertaining to return match photographs, and the final result of the investigation. These records should be maintained for a minimum of ten years to allow for future studies on FRT programs.

As the general public becomes aware of FRT applications being made readily available for department members, an influx of FOIA requests is likely to occur. To gain acceptance from the public, departments shall have extensive records that can be released to citizens upon request. This will allow the general public to arrive at their own conclusions after being informed of all the facts. The absence of a comprehensive process for record keeping may sow doubt amongst the populace, which could have a negative outcome for agencies attempting to introduce FRT programs.

Policy creation discussion. FRT has the ability to alter police investigations in a manner not observed since the introduction of DNA evidence. No longer will police need to release an image of a suspect to the media, hoping that someone from the community will come forward and assist in their identification. In large urban areas with a significant prevalence of violent crimes, these cases often see minimal media coverage. Soon officers will have the ability to submit a still photograph from a surveillance or doorbell camera, generating leads to the identification and arrest of offenders. In the words of Voltaire, "with great power comes great responsibility." This is where the necessity of a robust and meticulous policy governing the usage of such a powerful

technology is born. Members of the public, including this author, are often skeptical of relinquishing aspects of their privacy to government officials. The knowledge that stringent standards govern this technology's existence may pacify these concerns.

The World Economic Forum recommends incorporating nine principles into a responsible FRT policy. Incorporating these principles should be used as the building blocks of a policy that will garner input and trust from the public whom these law enforcement agencies serve. These principles are shown below with an overview of this author's commentary on the definition and importance of each. (WEF, 2021):

Respect for human and fundamental rights. This principle should be considered paramount and the birthing place for all FRT policies. As discussed throughout this research project, U.S. citizens are protected through several fundamental rights outlined in the U.S. Constitution. Facial recognition is a powerful tool that may be viewed as teetering on the fence of violating the privacy rights of individual persons or groups.

Any FRT policy should include provisions that forbid the use of FRT on any persons or groups practicing their First Amendment rights to free speech. In addition, the policy should include language similar to that found in the Detroit P.D. policy, banning the usage of this technology based on a person's religious, social, or political views; participation in a lawful event; and characteristics such as race, ethnicity, gender, disabilities, or sexual orientation. These policies shall also consider and account for issues that may arise in connection with the Fourth Amendment. For example, while courts have ruled extensively on a person's lack of an expectation of privacy in certain public places, this author believes this aspect will provide the most significant hurdle to public acceptance.

Necessary and proportional use. This principle acts as a balancing test between the need to identify the individual and the individual's rights. Usage of real-time FRT and the utilization of publicly available photographs need to be addressed. A stringent set of restrictions should be applied to real-time FRT usage. Exceptions should account for instances in which a real and present danger exists to the public or individual. Examples of these instances should be provided, such as finding a suspect who has committed a violent act of terrorism or locating a missing or kidnapped child.

Departments would be wise to restrict the outcomes in which these exceptions are allowed to avoid the fruit of the poisonous tree-type scenarios. For instance, an agency has been granted access to real-time FRT under the guise of locating a missing child; during this process, a person is located with a misdemeanor warrant. Department personnel should be forbidden from taking action or making an arrest on the warrant.

The issue of how or where the agency or third-party vendor obtains photographs for comparison analysis requires scrutiny. A policy should specify the databases utilized within the FRT program and the instances in which the agency would be allowed to deviate from said restrictions. For example, should an agency be limited to booking photos? Should an agency have access to DMV databases? Images scraped from the internet? Once again, a clearly defined set of standards will be a tremendous asset upon presentation to the public.

Transparency. Transparency and recordkeeping are the foundation for accountability. This author has discussed the importance of recordkeeping earlier in this report. Information such as program usage and requests, outside vendor participation, and photograph databases should be made public upon request and published in quarterly reports available for public viewing. To protect the privacy and integrity of specific cases, certain data should remain private or offered in a redacted version, stripping away any identifying characteristics. At a minimum, these reports should include:

- The officer making the request
- The Uniform Crime Report (UCR) number of specific cases requesting FRT (the UCR is a program in which the FBI compiles crime statistics data across the United States)
- Number of total FRT requests from agency members
- Average number of return images within a specific similarity score range
- Percentage of cases that have been resolved by arrest where the program identified the subject in question as the primary return image
- Number of cases where the top similarity score was not identified as the person wanted
- Number of cases where no images were returned as likely matches
- Number of FRT searches conducted within the department and number conducted by outside vendors
- Database where return images were located (booking photo, DMV photo, FBI database)

Human oversight and accountability. To achieve this principle, an agency will need to incorporate multiple levels of redundancy and supervisory approval. This author suggests a process that might involve a member requesting the usage of FRT programs to complete a departmental form explaining in detail the purpose of the request and particulars of the investigation. This form should be reviewed and approved by the member's immediate supervisor and bureau or section supervisor. Once approval is granted, a supervisor of the FRT program shall review and approve the form before the request is eventually sent to the unit member who will conduct the FRT process.

Upon completion of the analysis, the results shall be confirmed by blind verification of a second facial expert facial examiner. The supervisor of the FRT unit will then review these results before eventually being returned to the requesting investigator. The requesting investigator will review these results before any additional law enforcement action is taken.

System performance. The WEF suggests that agencies follow specific standards to ensure the accuracy of the algorithms designed and employed by their vendors and ensure vendors submit their algorithms for independent testing. To satisfy this requirement, an agency that contracts their FRT programs to third party vendors shall include a stipulation in the memorandum of agreement that any and all algorithms used by said vendor are submitted to and meet all standards as required by NIST and/or the FBI. Departments that may conduct their own FRT analysis should also specify which algorithms are being utilized as well as the date on which the algorithm was deemed

acceptable by NIST or the FBI. The policy should also include expiration dates for each algorithm, thus requiring recertification from the NIST or FBI.

Risk mitigation strategies. WEF states that departments should deploy risk mitigation processes to identify, monitor, and mitigate the risks of error and biases throughout the system's entire life cycle. This author believes this principle is directly intertwined with system performance. For example, requiring that algorithms meet the standards set forth by NIST and the FBI will account for the risk of errors or biases. Additionally, requiring members to verify returned match photographs through a multi-layered process will minimize harm to those persons or groups that may experience a higher percentage of discrepancy in Rank 1 accuracy returns.

Training of facial examiners. Prior to introducing an FRT program, a department will need to set training standards and protocols. This author suggests that a yearly training program be established that will require attendance from any member that requests or conducts facial recognition searches.

Use of probe images and reference databases. Departments should include in their policy which databases images will be retrieved from. This section shall also include any restrictions placed on certain databases and the specific circumstances in which this restriction can be circumvented.

Image and metadata integrity. WEF recommends this principle to mitigate the risk of errors from the submission of poor-quality probe photographs. An FRT policy should include minimum standards for quality and pose that will be collected for investigative use. Again, any allowances for deviation from set standards need to be clearly defined and accounted for by the investigating officer.

Recommendations

Facial recognition and its technology are evolving at a rapid pace. As a result, law enforcement agencies will need to create a living document that will be constantly reviewed and updated to remain relevant and practical. It will become imperative for agencies to seek input from all relevant stakeholders in an open and transparent manner to accomplish this goal. FRT has the ability to become an effective tool assisting law enforcement agencies conducting investigations but may become a thorn in the side of an agency if these programs are thought to operate in a shadowy manner.

This author feels that if the following recommendations are implemented, FRT usage from law enforcement will see a higher rate of acceptance amongst the public, current FRT programs will be strengthened, newly established FRT programs will become effective, and the technology will meet the standards to become admissible in a court of law.

Recommendation 1: Invoke Stakeholder Involvement

One of the biggest challenges to implementing an FRT program could be pushback from the general public. In order to reassure constituents and other relevant stakeholders, it will become imperative to integrate these groups into the process from the ground floor. These meetings will serve to satisfy numerous needs and concerns regarding the implementation of an FRT program. The relevant stakeholders will most likely include a diverse group of individuals such as:

- Members of the general public
- Members of the law enforcement community
- Members from third-party facial recognition vendors
- Local and state politicians
- Members of the legal community, including prosecutors, defense attorneys, and judges
- Facial examiners considered experts in their field
- Members of academia

This working group can serve a multitude of purposes. First, law enforcement officers will have the ability to directly address the public concerns while explaining in detail the expected outcomes of installing an FRT program. The feedback from these two groups is pivotal in the decision-making process. For example, agencies may learn that the public is deeply concerned about utilizing photographs obtained by non-law enforcement entities. To appease these concerns, agencies may decide to include provisions in this policy that will restrict access to certain types of photos.

A second important takeaway from this method of interaction is that this will be the optimal time to educate members of the public and local and state politicians on what FRT is and what it is not.

Third-party vendors and expert facial examiners will have the opportunity to address various areas of concern while detailing the benefits and limitations of this technology. In addition, legal experts can contribute their knowledge of the law, describing the instances where the usage of FRT is allowed or prohibited. These stakeholder meetings will serve as the linchpin to gaining the acceptance of the local populace and other community members.

Recommendation 2: Create a Working Group

Prior to stakeholder meetings, an agency shall create a working group comprised of members that will be responsible for the creation and implementation of the FRT program. Several topics will need to be addressed, such as:

- Determining the primary objectives and expected/desired outcomes
- Becoming familiar with local ordinances and state laws
- Researching the pros/cons of conducting the program within the agency vs. contracting the program out to third-party vendors
- Cost analysis and methods for securing funding
- Researching training options for agency members

Upon completing several public meetings to garner feedback from relevant stakeholders, the agency should begin to operate with a more precise end goal. At this time, the group should finalize the topics listed above. During this process, finalizing the primary objectives and expected/desired outcomes will be the foremost objective. In addition, measurement tools will need to be identified that will allow the agency to determine if its program is effective once it becomes operational.

For example, an agency needs to have the capability to track statistics that will be helpful in attaining their expected/desired outcomes. In near real-time, an organization should be able to view data concerning the following topics:

- Number of FRT requests
- Average number of return images
- Percentage of cases that resulted in an arrest or case being considered closed as a result of an FRT image return
- Percentage of cases where no return image was found or cases where the returned image was not related to the suspect

To accomplish this goal, the agency will need to develop a stringent recordkeeping system which will also serve as a method of creating transparency, as these results could be readily available to the public upon request.

Recommendation 3: Create a Training Program

It is recommended that any agency that utilizes an FRT program create and implement a stringent training program for any and all agency members involved in the FRT process. This training shall be conducted on an annual basis. This program, at minimum, should address the following criteria:

- The types and quality of photographs necessary to conduct facial recognition analysis
- Instances in which FRT requests are permissible and restricted
- Overview of the First and Fourth Amendments
- Explanation of the process of requesting FRT
- The next steps of an investigation upon return images and the necessity to confirm the suspect's identity through other means

Additionally, those members of the agency that will be conducting FRT analysis shall go through a rigorous training program in which they will become certified expert facial examiners. The author is aware that budget constraints will force some, if not most, departments or agencies to contract this process to third-party vendors. In this instance, it will become imperative that the department has access to the training records of vendor employees and the process in which the analysis is conducted.

Recommendation 4: Finalize and Implement Policy

Upon receiving the feedback from relevant stakeholders, creating a working group within the agency, and creating a training program, an agency will now be ready to finalize and implement its FRT program and policy. This document should be reviewed, at minimum, on an annual basis to allow for changes to the policy to adhere to advancements in facial recognition technology, new or changing legislature, and court rulings pertaining to legal challenges to the inclusion of this technology into criminal cases.

To assist agencies in pursuing the implementation of an FRT program, this author has created a policy template located in Appendix A of this report. This policy was created utilizing the nine principles suggested by WEF and discussed above. This template will consist of the following sections:

1. **Purpose Statement:** States the purpose of the policy
2. **Scope:** Defines the information included in the policy
3. **Glossary:** List of commonly used definitions and acronyms
4. **Procedures:** Details the specific procedures for obtaining and submitting photographs, the process for which match photographs are confirmed, and investigative next steps.

5. **Roles / Responsibilities:** Provides a detailed list of roles and responsibilities for stakeholders participating in the FRT program.
6. **Authorizations and Prohibitions:** A clearly defined set of circumstances in which the use of FRT is allowed or prohibited. This section should also include the exceptions to this rule.
7. **Reporting / Recordkeeping:** Outline the recordkeeping process and state the minimum time requirements for retention.
8. **Training:** An overview of the training program and the minimum standards that employees must meet.
9. **Accountability and Enforcement:** Describe the disciplinary process for employees who violate the standards outlined in this policy.

This template was created with information gathered from the standards outlined in documents released by the DOJ, the policies examined for this study, WEF, and the IACP. The combination of the above material will assist in creating what this author contends will become a reliable FRT policy that can then be adopted and modified to meet the needs of a specific law enforcement agency.

Conclusion

In conclusion, this research paper discussed the multiple aspects of Facial Recognition Technology. A brief history was given, along with an overview of how FRT operates and its many applications being used in law enforcement agencies and private sector settings. This paper examined new and existing laws at the state, local, and federal levels. Concerns of civil rights activists, limitations of FRT, and possible misuse were detailed. Confrontations Clause, Hearsay ruling, the Federal Rules of Evidence and Fourth Amendment implications were discussed. current police department FRT policies were documented.

The objectives from this research highlight the forthcoming legal challenges that may present as FRT utilization expands into criminal court proceedings. Suggestions for implementation of an FRT program that will survive the inevitable legal challenges ahead were given. This project culminates in a policy template that can be adopted by law enforcement agencies that will assist in compliance with federal, state, and local laws.

Implications

FRT can assist law enforcement officers in preventing acts of mass destruction (Hoffman, 2020). Unfortunately, the lack of a standardized industry-accepted best practice policy and procedures has accelerated lawmakers' decisions to create and pass "knee-jerk" legislation that may hinder law enforcement for decades to come (Claughton, 2019). Upon completion of this project, an FRT policy was created that will ensure conformity with laws and regulations, predict the legal challenges this technology will face once it becomes more prominent in the legal setting, and mandate that law enforcement officials act in a professional and legal manner (Orrick, n.d.).

Furthermore, this policy will ensure that citizens' civil liberties are protected through stakeholder involvement in the creation of the policy and the ability to participate at regular policy review sessions. Finally, a fair, consistent, and transparent policy will benefit law enforcement agencies and the general public as criminals are more easily identified and removed from the streets while law-abiding citizens enjoy their rights to privacy.

Suggestions for Future Research

Further research is needed to examine negative and positive outcomes from departments utilizing FRT. One research model would include conducting a long-term study that would examine departments' compliance with established best practice methods to ensure departments are operating inside the parameters set forth by legislators.

A measurement tool should be included to determine the validity of FRT procedures to examine the worthiness of this technology in comparison to its cost-effectiveness and possible negative perceptions of the general public. Additional research should also be conducted as FRT is introduced into the courtroom. Legal challenges will most likely arise, at which time court rulings will define the legal standards.

References

- 28 U.S.C. 702 – Testimony by Experts.
- A.B. 1215, Law enforcement: facial recognition and other biometric surveillance. 2019-20 Reg. Sess.(Cal,2019).https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=20192000AB1215
- AAMVA. (2019). *Facial recognition program: Best practice*. American Association of Motor Vehicle Administrators.
- ACLU(a). (2020, August 4). *Face recognition technology*. American Civil Liberties Union. <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology>
- ACLU(b). (2020, September 11). *Stopping face recognition surveillance*. American Civil Liberties Union. <https://www.aclu.org/news/topic/stopping-face-recognition-surveillance/>
- An Act Relative to Justice, Equity, and Accountability in Law Enforcement in the Commonwealth of 2020 Reg. Sess. (Mass, 2020)S.2963, 192nd General Court.
- Amazon Web Services. (n.d.) Compare Faces. https://docs.aws.amazon.com/rekognition/latest/dg/API_CompareFaces.html
- Amazon. (n.d.). *Use cases that involve public safety*. Amazon Web Services. <https://docs.aws.amazon.com/rekognition/latest/dg/considerations-public-safety-use-cases.html>
- Andenas, M., & Fairgrieve, D. (2012). Intent on making mischief: Seven ways of using comparative law. In P. G. Monateri (Ed.), *Methods of comparative law* (pp. 25–60). Edward Elgar Publishing.
- Anderson, J. E. (2003). *Public policymaking: An introduction*. Houghton Mifflin College Division.
- Anyebe, A. (2018). An overview of approaches to the study of public policy. *International Journal of Political Science (IJPS)*, 4(1), 8-17. <https://www.arcjournals.org/pdfs/ijps/v4-i1/2.pdf>
- Bernson, S. (2009). Debating DNA collection. *National Institute of Justice*, (264), 9–13. <https://www.ojp.gov/sites/g/files/xyckuh241/files/archives/ncjrs/228383.pdf>
- Bonsor, K., & Johnson, R. (2001, September 4). *How facial recognition systems work*. HowStuffWorks. <https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm>
- Boston, Massachusetts, City Ordinance 16-62 § Ordinance Banning Face Surveillance Technology in Boston (2020).
- Brainard, R. (2020, September 24). *Smile! You're probably being filmed on camera!* KHAK. <https://khak.com/smile-youre-probably-being-filmed-on-camera/>
- BreifCam. (2020, September 14). *Facial recognition face recognition for safety, security & operational efficiency*. BriefCam. <https://www.briefcam.com/technology/facial-recognition/>
- Brice, S. (2020, November 15). A short history of facial recognition. *Medium*. <https://medium.com/the-innovation/4ecd290aaab1>
- Brown, L. (2019, November 12). There will be no turning back on facial recognition. *Intelligencer*. <https://nymag.com/intelligencer/2019/11/the-future-of-facial-recognition-in-america.html>

- Brown, R. (2018, March 21). A Florida drug case could set precedent for facial recognition in policing. *New York Daily News*. <https://www.govtech.com/public-safety/A-Florida-Drug-Case-Could-Set-Precedent-for-Facial-Recognition-in-Policing.html>
- Bullcoming v. New Mexico, 131 S. Ct. 2705, 2717 (2011).
- Bureau of Justice Assistance (BJA). (2017). *Face recognition policy development template: For use in criminal intelligence and investigative activities*. U.S. Department of Justice.
- Carpenter v. United States, 138 S. Ct. 2206 (2018).
- Carter, J., & Grommon, E. (2014, February). *Impact of mobile broadband data access on police operations: An exploratory case study of one medium-sized municipal police department*. Office of Justice Programs.
- Castro, D., & McLaughlin, M. (2019, September 10). *Banning facial recognition in police body cameras will make Californians less safe*. Information Technology & Innovation Foundation. <https://itif.org/publications/2019/09/10/banning-facial-recognition-police-body-cameras-will-make-californians-less>
- CBP(a). (2020). *Land*. U.S. Customs and Border Protection. <https://biometrics.cbp.gov/land>
- CBP(b). (2020, 12). *CBP introduces biometric facial comparison at Progreso Port of entry to secure and streamline travel*. U.S. Customs and Border Patrol. <https://www.cbp.gov/newsroom/local-media-release/cbp-introduces-biometric-facial-comparison-progreso-port-entry-secure>
- Celentino, J. (2016). Face-to-face with facial recognition evidence: Admissibility under the post-Crawford confrontation clause. *Michigan Law Review*, 114, 1317–1353.
- Chachere, V. (2006, January 7). Biometrics used to detect criminals at Super Bowl. *ABC News*. <https://abcnews.go.com/Technology/story?id=98871&page=1>
- Chappell, B. (2019, July 8). ICE uses facial recognition to sift state driver's license records, researchers say. *NPR.org*. <https://www.npr.org/2019/07/08/739491857/ice-uses-facial-recognition-to-sift-state-drivers-license-records-researchers>
- Charmaz, K. (2000). Grounded theory: objectivist and constructivist methods. In *Handbook of qualitative research* (2nd ed., pp. 509–535). Sage.
- Charmaz, K. (2013). Grounded theory as an emergent trend. In *Handbook of emergent methods* (pp. 155–171). Guilford Publications.
- Ciresan, D., Meier, U., & Schmidhuber, J. (2012). Multi-column deep neural networks for image classification. *2012 IEEE Conference on Computer Vision and Pattern Recognition*.
- Claughton, E. (2019, August). Politics, records and facial recognition in criminal justice: How it affects us all. *Police Records Management*. <https://policerecordsmanagement.com/wp-content/uploads/2019/08/Politics-Records-and-Facial-Recognition.pdf>
- Conger, K., Fausset, R., & Kovalski, S. (2019, May 14). San Francisco bans facial recognition technology. *The New York Times*. <https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html>
- Cormier, K., Calandro, L., & Reeder, D. (2005). Evolution of DNA evidence for crime solving - a judicial and legislative history. *Forensics Magazine*, 2(4).
- Crawford v. Washington, 541 U.S. 36, 124 S. Ct. 1354 (2004).
- Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE.
- Crossey, N. (2020). Machine translator testimony & the confrontation clause: Has the time come for the hearsay rules to escape from the stone age? *Drexel Law Review*, 12, 561–

596. <https://drexel.edu/~/media/Files/law/law%20review/v123/Crossey%2012%20Drexel%20L%20Rev%20561.ashx>
- Crowe, S., Cresswell, K., Robertson, A., Hubry, G., Avery, A., Sheik, A (2011). The case study approach. *BMC Medical Research Methodology*, 11(100).
- CRS. (2020, October 27). *Federal law enforcement use of facial recognition technology*. Congressional Research Service. <https://fas.org/sgp/crs/misc/R46586.pdf>
- Daubert v. Merrell Dow Pharmaceuticals Inc., 509 U.S. 579, (1993).
- Davis v. Mississippi, 394 U.S. 721, (1969).
- Del Greco, K. (2019, June 4). *Facial recognition technology: Ensuring transparency in government use*. FBI. <https://www.fbi.gov/news/testimony/facial-recognition-technology-ensuring-transparency-in-government-use>
- DHS(a). (2020, July 13). *Biometrics*. Department of Homeland Security. <https://www.dhs.gov/biometrics>
- DHS(b). (2020, September 11). *All US states now compliant ahead of REAL ID deadline*. Department of Homeland Security. <https://www.dhs.gov/news/2020/09/10/all-us-states-now-compliant-ahead-real-id-deadline>
- DHS(c). (2020, May 13). *ICE use of facial recognition services*. Homeland Security. <https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-frs-054-may2020.pdf>
- Digital Justice Act of 2021, Portland, Oregon, Ordinance 190114, Code Title 34 §.
- District Attorney's Office for the Third Judicial District v. Osborne, 557 U.S. 52, 129 S. Ct. 2308 (2009).
- Dwivedi, D. (2019, March 27). Face detection for beginners. *Medium*. <https://towardsdatascience.com/face-detection-for-beginners-e58e8f21aad9>
- Eberle, E. J. (2009). The method and role of comparative law. *Washington University Global Studies Law Review*, 8(3).
- EFF. (2017, October 24). *Street-level surveillance*. Electronic Frontier Foundation. <https://www.eff.org/pages/facerecognition#>
- Ethical Use of Facial Recognition Act of 2020, S.3284 -116th Congress. Congress.gov. <https://www.congress.gov/bill/116th-congress/senate-bill/3284/text>
- Etikan, I., Musa, S., & Alkassim, R. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, 5(1), 1–4.
- Faceprint. (2020). In *Oxford Dictionary*. Oxford Languages.
- Facial Recognition Technology Act of 2020, Portland, Maine, Ord. 72-19/20 § Article XI.
- FBI. (2019). *Privacy impact assessment for the [Next Generation Identification-Interstate Photo System]*. Federal Bureau of Investigations.
- Frye v. United States, 293 F. 1013, D.C. Cir. (1923).
- GAO(a). (2020). *Facial recognition technology privacy and accuracy issues related to commercial uses* (GAO 20-522). United States Government Accountability Office. <https://www.gao.gov/assets/710/708045.pdf>
- GAO(b). (2020, September 2). *FACIAL RECOGNITION: CBP and TSA are taking steps to implement programs, but CBP should address privacy and system performance issues*. U.S. Government Accountability Office. <https://www.gao.gov/products/GAO-20-568>
- Gates, K. (2004, June). *Early research on machine recognition of faces*. University of Illinois at Urbana-Champaign. <http://www.acdis.uiuc.edu/research/OPs/Gates/contents/part2.html>

- Gates, K. (2011). *Our biometric future: Facial recognition technology and the culture of surveillance*. NYU Press.
- Gershgorn, D. (2020, June 2). *Exclusive: Live facial recognition is coming to U.S. police body cameras*. Medium. <https://onezero.medium.com/exclusive-live-facial-recognition-is-coming-to-u-s-police-body-cameras-bc9036918ae0>
- Ghaffary, S. (2019, December 10). *How to avoid a dystopian future of facial recognition in law enforcement*. Vox. <https://www.vox.com/recode/2019/12/10/20996085/ai-facial-recognition-police-law-enforcement-regulation>
- Glanton, D. (2019, February 26). *In a city with tens of thousands of surveillance cameras, who's watching whom?* chicagotribune.com. <https://www.chicagotribune.com/columns/dahleen-glanton/ct-met-dahleen-glanton-video-cameras-chicago-20190225-story.html>
- Greenberg, P. (2015). Automated license plate readers. *National Conference of State Legislators*, 23(8).
- Greenberg, P. (2020, September 18). *Facial recognition gaining measured acceptance*. Legislative News, Studies and Analysis | National Conference of State Legislatures. <https://www.ncsl.org/research/telecommunications-and-information-technology/facial-recognition-gaining-measured-acceptance-magazine2020.aspx>
- Grimes v. United States, 252 A.3d 901 (D.C. 2021)
- Guide to the confrontation clause. (2015). *The UNC School of Government: North Carolina Superior Court Judges' Handbook*, 2-37. https://www.sog.unc.edu/sites/www.sog.unc.edu/files/course_materials/02015.pdf
- Guliani, N. (2019, June 7). *The FBI has access to over 640 million photos of us through its facial recognition database*. American Civil Liberties Union. <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/fbi-has-access-over-640-million-photos-us-through#>
- Hamann, K., & Smith, R. (2019). Facial recognition technology: Where will it take us? *Criminal Justice Magazine*, 34(1). https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/
- Harwell, D. (2018, April 26). Facial recognition may be coming to a police body camera near you. *The Washington Post*. <https://www.washingtonpost.com/news/the-switch/wp/2018/04/26/facial-recognition-may-be-coming-to-a-police-body-camera-near-you/>
- Harwell, D. (2019, July 7). FBI, ICE find state driver's license photos are a gold mine for facial-recognition searches. *The Washington Post*. <https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/>
- Hern, A. (2021, January 27). Human rights group urges New York to ban police use of facial recognition. *The Guardian*. <https://www.theguardian.com/technology/2021/jan/25/new-york-facial-recognition-technology-police>
- Hoffman, A. (2020, March 9). Facial recognition could stop terrorists before they act. *The Hill*. <https://thehill.com/opinion/technology/486570-facial-recognition-could-stop-terrorists-before-they-act>
- Huffaker, S. (2016, June 10). How the FBI uses facial recognition technology to fight crime. *Newsweek*. <https://www.newsweek.com/2016/04/29/fbi-biometrics-facial-recognition-next-generation-identification-449146.html>

- Huhn, M. (2001, June 26). Just a face in the crowd? – Superbowl kicked off the use of face recognition software – but is this an invasion of privacy? *New York Post*. <https://nypost.com/2001/06/26/just-a-face-in-the-crowd-superbowl-kicked-off-the-use-of-face-recognition-software-but-is-this-an-invasion-of-privacy/>
- Ingber, S. (2019, June 27). Major police body camera manufacturer rejects facial recognition software. *NPR.org*. <https://www.npr.org/2019/06/27/736644485/major-police-body-camera-manufacturer-rejects-facial-recognition-software>
- Jany, L. (2021, January 22). Proposed ban on law enforcement facial recognition technology advances in Minneapolis. *Star Tribune*. <https://www.startribune.com/proposed-ban-on-use-of-facial-recognition-technology-by-police-advances-in-minneapolis/600013504/>
- Jones v. Murray, 962 F.2d 302 (4th Cir. 1992).
- Kaiser, J. (2019, November 7). A judge said police can search the DNA of 1 million Americans without their consent. What's next? *Science AAS*. <https://www.science.org/content/article/judge-said-police-can-search-dna-millions-americans-without-their-consent-what-s-next>
- Kamba, W. J. (1974). Comparative law: A theoretical framework. *International and Comparative Law Quarterly*, 23(3), 485–519.
- Kaste, M. (2018, May 10). Real-time facial recognition is available, but will U.S. police buy it? *NPR.org*. <https://www.npr.org/2018/05/10/609422158/real-time-facial-recognition-is-available-but-will-u-s-police-buy-it>
- Katz v. United States, 389 U.S. 347, 88 S. Ct. 507 (1967).
- Keene, P. (2020, October 8). So far, three U.S. cities have banned facial recognition software. *Klemchuk LLP*. <https://www.klemchuk.com/ip-law-trends/cities-ban-facial-recognition-software-in-public>
- Kelley, J. (2020, March 19). Announcing who has your face. *Electronic Frontier Foundation*. <https://www.eff.org/deeplinks/2020/03/announcing-who-has-your-face>
- Kershner, E. (2020, August 3). The largest police departments in the US. *WorldAtlas*. <https://www.worldatlas.com/articles/the-largest-police-departments-in-the-us.html>
- Klosowski, T. (2020, July 15). Facial recognition is everywhere. Here's what we can do about it. *Wirecutter: Reviews for the Real World*. <https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/>
- Kuhmo Tire Co. v. Carmichael, 526 U.S. 137, 119 S. Ct. 1167, 143 L. Ed. 2d 238, (1999). Law Enforcement Agency Policies and Procedures Regarding Video and Audio Recordings; Requirements; Exceptions Act of 2019, ORS § 133.741.
- Larmon, T. (2021). *A policy examination of digital multimedia evidence in police department standard operating procedures (SOPs)*. College of Education Theses and Dissertations. https://via.library.depaul.edu/soe_etd/214
- LeBlanc, P. (2019, July 8). Washington Post: ICE, FBI use state driver's license photos for facial-recognition scans. *CNN Digital*. <https://www.cnn.com/2019/07/08/politics/fbi-ice-driver-license-photos-facial-recognition/index.html>
- Li, S. Z., & Jain, A. K. (2005). *Handbook of face recognition*. Springer Science & Business Media.
- Lochner, S. (2013). Saving face: Regulating law enforcement's use of mobile facial recognition technology & iris scans. *Arizona Law Review*, 55(201), 202–233.
- Lockheed Martin. (2014, September 18). *Lockheed Martin team helps bring FBI's next generation identification to full operational capacity*. Media - Lockheed

- Martin. <https://news.lockheedmartin.com/2014-09-18-Lockheed-Martin-Team-Helps-Bring-FBIs-Next-Generation-Identification-To-Full-Operational-Capacity>
- Louradour, S., & Madzou, L. (2021). A policy framework for responsible limits on facial recognition: Use case: law enforcement investigations. *World Economic Forum*.
- Lydick, N. (n.d.). *A brief overview of facial recognition*. Electrical Engineering and Computer Science at the University of Michigan. <https://www.eecs.umich.edu/courses/eecs487/w07/sa/pdf/nlydick-facial-recognition.pdf>
- Lynch, J. (2020, April 20). Face off: Law enforcement use of face recognition technology. *Electronic Frontier Foundation*. <https://www.eff.org/wp/law-enforcement-use-face-recognition>
- Lynch v. State, 260 So. 3d 1166 (Fla. Dist. Ct. App. 2018).
- Maryland v. King, 569 U.S. 435, 133 S. Ct. 1958, 186 L. Ed. 2d 1, 24 Fla. L. Weekly Supp. 234, (2013).
- Mattox v. United States, 156 U.S. 237, 242-43 (1895).
- Merriam-Webster. (n.d.). *Definition of policy*. Dictionary by Merriam-Webster: America's most-trusted online dictionary. <https://www.merriam-webster.com/dictionary/policy>
- Miller, J. (2015, May 13). *FBI delivers on \$1.1B biometrics program*. Federal News Network. <https://federalnewsnetwork.com/technology-main/2015/05/fbi-delivers-on-11b-biometrics-program/>
- Miller, J. (2019, May 9). Face detection vs. Face recognition: What's the difference? *FaceFirst Face Recognition Software*. <https://www.facefirst.com/blog/face-detection-vs-face-recognition/>
- Mills, J., Bonner, A., & Francis, K. (2006). Adopting a constructivist approach to grounded theory: Implications for research design. *International Journal of Nursing Practice*, 12(1), 8–13.
- Moenssens, A., & Meagher, S. (2014). Fingerprints and the law. In United States Department of Justice (Ed.), *The fingerprint sourcebook*. CreateSpace. Chapter 13.
- Moses, K. (2014). Automated fingerprint identification system. In United States Department of Justice (Ed.), *The fingerprint sourcebook*. CreateSpace. Chapter 6.
- Napolitano v. United States, 340 F.2d 313, 314, (1st Cir.'65).
- National Biometric Information Privacy Act of 2020, S. 4400-116th Congress. Congress.gov. <https://www.congress.gov/bill/116th-congress/senate-bill/4400/text>
- New York v. Class, 475 U.S. 106, 113 (1986).
- NH Rev Stat § 105-D:2 (2016).
- Nilsson, N. J. (2009). *The quest for artificial intelligence*. Cambridge University Press.
- NIST. (2018, December 6). NIST evaluation shows advance in face recognition software's capabilities. *National Institute of Standards and Technology*. <https://www.nist.gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-software-capabilities>
- Norman, J. (n.d.). *Woodrow Bledsoe originates of automated facial recognition: History of information*. <https://www.historyofinformation.com/detail.php?entryid=2495>
- Ohio v. Roberts, 448 U.S. 56, 100 S. Ct. 2531 (1980).
- Olmstead v. United States, 277 U.S. 438, 48 S. Ct. 564 (1928).
- Orrick, W. (n.d.). *Developing a police department policy-procedure manual*. International Association of Chiefs of Police. <https://www.theiacp.org/sites/default/files/2018-08/BP-PolicyProcedures.pdf>

- O'Sullivan, D. (2019, August 19). Bernie Sanders wants to stop police from using facial recognition software. *CNN Digital*. <https://www.cnn.com/2019/08/19/tech/bernie-sanders-facial-recognition-police/index.html>
- Panda Security. (2020, October 13). *The complete guide to facial recognition technology*. Panda Security Mediacenter. <https://www.pandasecurity.com/en/mediacenter/panda-security/facial-recognition-technology/>
- Paris, M. (2016). The comparative method in legal research: The art of justifying choices. In L. Cahillane & J. Schweppe (Eds.), *Legal research methods: Principles and practicalities*.
- Parker, J. (2020, December 10). Facial recognition success stories showcase positive use cases of the technology. *Security Industry Association*. <https://www.securityindustry.org/2020/07/16/facial-recognition-success-stories-showcase-positive-use-cases-of-the-technology/>
- Pasley, J. (2019, December 6). I documented every surveillance camera on my way to work in New York City, and it revealed a dystopian reality. *Business Insider*. <https://www.businessinsider.com/how-many-security-cameras-in-new-york-city-2019-12>
- Patidar, J. (2013, May 7). Non-experimental research design. <https://www.drjayeshpatidar.blogspot.com>
- People v. Jennings, 252 Ill. 534 (IL. Sup Ct. 1911).
- People v. John, 27 N.Y.3d 294, (2016).
- People v. Reyes, N.Y. Slip Op. 20258 (N.Y. Sup. Ct. 2020).
- People v. Wesley, 83 N.Y.2d 417, 422 (1994).
- Perry, W., McInnis, B., Price, C., Smith, S., & Hollywood, J. (2013). *Predictive policing: The role of crime forecasting in law enforcement operation*. Rand Safety and Justice Program.
- Petrov, M. (2012). *Law enforcement application of forensic face recognition*. Biometric news Biometric Information | Planet Biometrics. https://www.planetbiometrics.com/creo_files/upload/article-files/whitepaper_facial_recognition_morphotrust.pdf
- Phillips, P. J., Flynn, P. J., Bowyer, K. W., Bruegge, R. W., Grother, P. J., Quinn, G. W., & Pruitt, M. (2011). Distinguishing identical twins by face recognition. *Face and Gesture*.
- Phillips, P., Moon, H., Rizvi, S., & Rauss, P. (1999, January 7). *The FERET evaluation methodology for face-recognition algorithms*. TSAPPS at NIST. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=900863
- Ravitch, S. M., & Carl, N. M. (2015). *Qualitative research: Bridging the conceptual, theoretical, and methodological* (1st ed.). SAGE.
- Raviv, S. (2020, January 21). The secret history of facial recognition. *Wired*. <https://www.wired.com/story/secret-history-facial-recognition/>
- Reitz, J. C. (1998). How to do comparative law. *The American Journal of Comparative Law*, 46(4), 617.
- Ridder, H. (2017, February 16). The theory contribution of case study research designs. *Business Research*. <https://link.springer.com/article/10.1007/s40685-017-0045-z>
- S.B. 6280, 66th Legislature, 2020 Reg. Sess. (Wash, 2020). <http://lawfilesexxt.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Passed%20Legislature/6280-S.PL.pdf#page=1>
- Sample, I. (2019, July 29). What is facial recognition - and how sinister is it? *The Guardian*. <https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it>

- San Francisco, California, Administrative Code sec. 19B § Acquisition of Surveillance Technology (2019).
- Schuppe, J. (2018, July 30). Facial recognition gives police a powerful new tracking tool. It's also raising alarms. *NBC News*. <https://www.nbcnews.com/news/us-news/facial-recognition-gives-police-powerful-new-tracking-tool-it-s-n894936>
- Shepley, A. (n.d.). *Deep face learning for face recognition: A critical analysis*. arXiv.org e-Print archive. <https://arxiv.org/ftp/arxiv/papers/1907/1907.12739.pdf>
- Sites, B. (2020). The future of the Confrontation Clause: Semiautonomous and autonomous machine witnesses. *Vanderbilt Journal of Entertainment and Technology Law*, 22(3), 547–585.
- Smith, R. (2019, June 27). *The future of face matching at axon and AI ethics board report*. Protect Life | Axon. <https://www.axon.com/company/news/ai-ethics-board-report>
- Smith v. United States, 324 F.2d 879, 882, D.C. (Cir. 1963).
- Solon, O. (2019, March 17). Facial recognition's 'dirty little secret': Social media photos used without consent. *NBC News*. <https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921>
- State v. Cerciello, 86 N.J.L. 309, 90 Atl. 1112 (GA. 1914)
- State v. Dabney, 2003 WI App 108; 264 Wis. 2d 843; 663 N.W.2d 366 (WI. 2003).
- State v. Ortiz-Zape, 743 S.E.2d 156, 367 N.C. 1 (N.C. 2013).
- State v. Reinhardt, 875 N.W.2d 25, 2016 S.D. 11 (S.D. 2016)
- Stacy v. State, 49 Okl. Crim. 154, 292 P. 885 (OK. 1930)
- Street, F. (2019, October 8). How facial recognition is taking over airports. *CNN*. <https://www.cnn.com/travel/article/airports-facial-recognition/index.html>
- Stroud, M. (2016, July 18). Taser plans to Livestream police body camera footage to the cloud by 2017. *VICE*. <https://www.vice.com/en/article/4xa43g/taser-axon-police-body-camera-livestream>
- Syafeeza, A., Khalil-Hani, M., Liew, S., & Bakhteri, R. (2014). Convolutional neural network for face recognition with pose and illumination variation. *International Journal of Engineering and Technology*, 6(1), 44–57.
- Taylor, D. (n.d.). How facial recognition technology is being used at airports. *Travel Market Report: The Voice of The Travel Advisor*. <https://www.travelmarketreport.com/articles/How-Facial-Recognition-Technology-is-Being-Used-at-Airports>
- Taherdoost, H. (2018). A review of technology acceptance and adoption models and theories. *Procedia Manufacturing*, 22, 960–967.
- Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research*, 6(2), 144–176.
- Thorkildsen, Z., Wohl, E., Bryson, B., Lafferty, J., & Dockstader, J. (2019, December). *Common operational picture technology in law enforcement: Three case studies*. Office of Justice Programs. <https://www.ojp.gov/pdffiles1/nij/grants/254624.pdf>
- Top 10 largest sheriff's departments in the United States! (2020, August 8). *Police Test Study Guide*. <https://policeteststudyguide.com/largest-sheriffs-departments-in-the-united-states/>
- U.S. Const. amend. IV.
- U.S. Const. amend. VI.
- United States v. Jones, 908 F. Supp. 2d 203 (D.D.C. 2012).
- United States v. Kelly, 55 F.2d 67, 2d Cir. (1932).

- United States v. Knotts, 460 U.S. 276, 280 (1983).
- United States. (2014). Article VII. Hearsay: The federal rules of evidence.
- University of Southern Denmark Library. (n.d.). *Better thesis your online support*. University of Copenhagen. <http://betterthesis.dk/research-methods>
- Viola, P., & Jones, M. (2004, May). Rapid object detection using a boosted cascade of simple features. *ResearchGate*.
https://www.researchgate.net/profile/Michael_Jones20/publication/3940582_Rapid_Object_Detection_using_a_Boosted_Cascade_of_Simple_Features/links/0f31753b419c639337000000.pdf
- Wagner, I. (2020, February 26). Licensed drivers in the U.S. - total number by state 2018. *Statista*. <https://www.statista.com/statistics/198029/total-number-of-us-licensed-drivers-by-state/>
- Wang, J., & Li, Z. (2018). *Research on face recognition based on CNN*. School of Electrical Engineering, Zhengzhou University.
- Ward, K., Chibnall, S., & Harris, R. (2007). *Measuring excellence: Planning and managing evaluations of law enforcement initiatives*. Inner City Fund International.
- Washington v. Griffin, 876 F.3d 395 (2d Cir. 2017).
- Westrope, A. (2020, March 23). *Wolfcom embraces body cam face recognition despite concerns*. Government Technology State & Local Articles - e.Republic. <https://www.govtech.com/biz/Wolfcom-Embraces-Body-Cam-Face-Recognition-Despite-Concerns.html>
- Whorton v. Bockting, 549 U.S. 406, 127 S. Ct. 1173 (2007).
- Williams v. Illinois, 567 U.S. 50, 132 S. Ct. 2221, 183 L. Ed. 2d 89, (2012).

Appendix A: Sample Policy

Purpose Statement

The purpose of this document is to establish guidelines for the usage of facial recognition technology (FRT) programs within the [*Sample Law Enforcement Agency*]. The FRT policy includes standard operating procedures (SOPs) for utilizing facial recognition during criminal investigations. All deployments of the face recognition system are for official use only/law enforcement sensitive (FOUO/LES).

Scope

FRT examines and compares distinguishing characteristics, or nodal points, of a human face through the utilization of biometric algorithms contained within a software application. This technology can be a valuable investigative tool and assist a law enforcement agency identify and locate criminals, locate missing persons, and provide large-scale event security.

Procedures

When an investigator obtains an image depicting the face of an unidentified suspect, victim, or witness, and intends to identify the individual using facial recognition technology, which includes any digital comparison of the probe image to photos stored in the photo repository, the assigned investigator must submit a request to the unit within the agency tasked with operating the

Assigned Investigator

1. Obtain image of individual to be identified.
 - a. If video is submitted, include associated software/player.
 - b. If image is from internet/social media, include site link.
2. Complete pertinent forms and upload image to the assigned program.

Immediate Supervisor

3. Confirm underlying basis for request is in compliance with authorized uses of facial recognition technology.
 - a. Document confirmation and forward request to supervisor of unit conducting FRT program.

FRT Supervisor

4. Confirm underlying basis for request is in compliance with authorized uses of facial recognition technology.
 - a. Assign request to facial recognition examiner.

Facial Recognition Examiner

5. Select probe image of individual to be identified from images submitted.
 - a. Trained examiners will initially run probe images without filters, using a filtered search as a secondary search, if needed. In some cases, enhancements may be considered after running an image as is against the image repository.
 - b. In the automated search, most likely candidates are returned to the requestor ranked in order based on the similarity or confidence level.
 - c. If image quality is unsuitable for facial recognition comparison, notify the assigned investigator departmental email.
 - d. Permit assigned investigator to submit additional images.
6. Run query using facial recognition technology for comparison of probe image to images stored in photo repository, and generate pool of possible match candidates.
7. The resulting candidates, if any, are then manually compared with the probe images and examined by an authorized, trained examiner. Examiners shall conduct the comparison of images, biometric identifiers, and biometric information in accordance with their training. If no likely candidates are found, the requesting entity will be informed of the negative results. In the case of a negative result, the images examined by the examiner will not be provided to the requesting entity.
8. Perform detailed background check to confirm reliability of match, if possible match candidate is identified.
9. Examiners will submit the search and subsequent examination results for a peer review of the probe and candidate images for verification by other authorized, trained examiners

FRT Supervisor

10. Conduct final review of possible match candidate, and approve, if appropriate.
11. Direct facial recognition examiner investigator to provide possible match candidate to assigned investigator if in agreement with findings.
12. Direct facial recognition examiner to continue investigation for possible match candidate, if not in agreement with findings of facial recognition examiner.
 - a. Direct facial recognition examiner to report negative results to assigned investigator report, if possible match candidate is not identified or approved by supervisor.

Facial Recognition Examiner

13. Prepare report and upload to assigned investigator's case file, if supervisor confirms possible match candidate.

- a. Report shall include probe image, and notification stating that determination of a possible match candidate alone does not constitute probable cause to effect an arrest, or obtain an arrest or search warrant, and that further investigation is needed to establish probable cause.

14. Retain all records of facial recognition searches, including associated case file number, reason each search was requested, details, and search results, and upload them into the case file.

Assigned Investigator

15. Conduct further investigation to determine whether possible match candidate is connected to, or involved in, incident under investigation, upon receipt of report in order to establish probable cause.

16. Continue investigation, (i.e., obtaining additional suitable images for another submission), if no possible match candidate was determined, or image was rejected.

Roles/Responsibilities

Assigned Investigator: Is the individual responsible for the investigation. This person will be responsible for obtaining and selecting the probe image for comparison. The final results of the investigation will be the responsibility of the assigned investigator.

Immediate Supervisor: This individual will act as the immediate supervisor to the assigned investigator. They will ensure all requests are documented properly, and all requests fit within the guidelines delineated in this policy.

FRT Supervisor: Individual will be responsible to ensuring all requests are documented according to policy and procedures. FRT Supervisor will also ensure all requests fit within the guidelines delineated in this policy. This person will assign requests to facial recognition examiners. FRT Supervisor will monitor the FRT process and be responsible for conducting final review of possible match candidate, and approve, if appropriate. FRT supervisor is responsible for documenting and recordkeeping of all facial recognition requests.

Facial Recognition Examiner: Individual will be responsible for operating the program selected by the agency. This person will examine possible match photographs and determine possible match candidates based on similarity scores. Facial recognition examiners will also submit their findings to other facial recognition examiners for peer-review before submitting final results to FRT supervisor.

Authorizations and Prohibitions

Facial recognition technology shall be used for official law enforcement purposes to include, but not limited to:

- a. Ascertaining the identification of individual that has committed a criminal offense and where an investigator deems there is sufficient probable cause to warrant the use of facial recognition.
- b. An active or ongoing criminal investigation.
- c. To mitigate an imminent threat to health or safety.
- d. To assist in the identification or locating or missing or high-risk persons.
- e. To investigate and/or corroborate tips and leads.
- f. To support law enforcement in critical incident responses.

Facial recognition technology shall be used not used for:

- a. Personal use, queries not related to legitimate agency duties, sharing, copying, or passing of information to unauthorized personnel.
- b. Any purpose that violates the U.S. Constitution or laws of the United States, including protections of the First, Fourth, and Fourteenth Amendments.
- c. Harassing and/or intimidating any individual or group.
- d. Any other access, use, disclosure, or retention that would violate applicable law or agency policy.
- e. Facial recognition technology cannot be used to conduct surveillance of persons or groups based solely on their religious, political or other constitutionally protected activities, their race, ethnicity, gender, or sexual orientation.
- f. Prohibiting or deterring lawful individual exercise of other rights, such as freedom of association, implied by or secured by the U.S. Constitution or any other constitutionally protected right or attribute.
- g. Members shall not use FRT to surveil the public through any camera or video device.

Reporting/Recordkeeping

All records will be stored in a central location. The agency will conduct an audit of the facial recognition program on a monthly basis by the immediate supervisor of the program. Audits will be conducted by top-level members of the agency on a semi-annual basis.

The agency will maintain an audit trail of requested, accessed, searched, or disseminated face recognition information. An audit trail will be kept for a minimum of ten years of requests, access, and searches of face recognition information for specific purposes and of what face recognition information is disseminated to each individual in response to the request. Audit logs will include:

- a. The name, agency, and contact information of the law enforcement user.
- b. The date and time of access.

- c. Case number.
- d. Probe images.
- e. The specific information accessed.
- f. The modification or deletion, if any, of the face recognition information.
- g. The authorized law enforcement or public safety justification for access (criminal investigation, criminal intelligence, imminent threat, or identification), including a relevant case number if available.
- h. The result of the return image (positive or negative), and the final disposition of that particular case number.

Training

FRT shall only be used by trained members who follow the procedures delineated in this policy. Every member within this organization that utilizes the facial recognition program should understand the capacities and limits of the system used. The training of examiners should include (but is not all inclusive):

- a. Updates of local, state, and federal regulations concerning the use of FRT.
- b. Review of specific court rulings that pertain to the usage of FRT in criminal investigations and the process that will ensure the admissibility of evidence resulting from the FRT programs.
- c. Members should be taught the process specific to the particular agency of the roles/responsibilities of each particular member during the collection, submission, and evaluation phases of the program.
- d. Members should be taught the risk of biases within the FRT program to include false positives and false negatives. Overview of the difference of performance on various demographics.
- e. Members should be made aware of the risk of image manipulation.
- f. Collection, storage, integrity and traceability of data processes.
- g. Human-machine interaction best practices.
- h. Members should be made aware of the ethics involved in utilizing an FRT program.
- i. Members shall be instructed on court testimony procedures.

Each member participating in the facial recognition program shall undergo training on an annual basis. Training modules will be updated annually to remain current and relevant.

If the agency contracts out facial recognition to a third-party non-governmental vendor, the agency shall enter into an agreement with said vendor to provide training to agency members.

Accountability and Enforcement

Accountability

An agency should make available to the public upon request information regarding the collection, access, use, dissemination, and retention practices. The agencies policy should be made accessible on the agency's website and available in print copy upon request.

The agency shall designate an individual responsible for responding to inquiries and Freedom of Information Act requests. This individual will be responsible for receiving complaints regarding incorrect information, privacy concerns, and system access.

Enforcement

An agency should adopt and follow procedures and practices to ensure and evaluate compliance of users with the FRT requirements and provisions of this policy and applicable law. This will include logging access to face recognition information, and will entail periodic random auditing of these systems. These audits will be mandated at least quarterly and a record of the audits will be maintained by the designated personnel pursuant to the retention policy. Appropriate elements of this audit process and key audit outcomes will be compiled into a report and may be provided to command staff and oversight entities or governance boards.

Members found to be in noncompliance with the provisions of this policy regarding the collection, receipt, access, use, dissemination, retention, will suspend or discontinue access to the authorized member.

An agency shall detail the disciplinary process to those members found to be in violation of the provisions of this policy.

Example Law Enforcement FRT Policy *Appendix A: Definitions*

Glossary

Audit - a review conducted by the department supervisors to include all use of facial recognition software/technology. The audit will include all user's activity, such as user log-ins and log-outs, each user's activity in detail, what commands were issued to the system, and what records or files were accessed.

Biometrics - body measurements and characteristics unique to an individual person that are utilized for automated recognition: e.g., fingerprints, palm prints, and iris scans.

Civil Rights - rights and privileges of equal protection that government entities must afford to all individuals in the United States regardless of race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, or other characteristics.

Examiner - An individual who has received training in the facial recognition system are qualified to assess image quality and appropriateness for facial recognition searches.

Facial recognition -broadly involves the automated searching of a facial image (a probe) against a known collection or database of photos.

Face Recognition Algorithm - consists of two parts (1) face detection and normalization and (2) face identification.

Facial Recognition Technology - computer systems that analyze images of human faces for the purposes of identifying them.

Faceprint - digital scan / photograph of a face that identifies an individual based on unique characteristics of the facial structure that is as unique to a specific person as a fingerprint.

False Positive - occurs when one or multiple suggested matches differ from the input image.

Investigative Lead - Information which could potentially aid in the successful resolution of an investigation but does not imply positive identification of an individual.

Negative Result -search of the probe image was not determined to be sufficiently similar to or resemble any of the reference images contained in an image repository.

Nodal points - various peaks and valleys that make up facial features, also referred to as landmarks. The human face consists of approximately 80 nodal points.

One-to-one verification - algorithms compare a photo of someone with a stored image of that known identity to determine if it is the same person.

One-to-many - algorithms compare features of a probe photo with all images of a database.

Peer Review - Examiners submit results to other authorized and trained examiners, or peers, for an independent review

Probability / Match Score - score given to the probability that one image matches another.

Probe photo - photograph of an individual that law enforcement officials are seeking to identify. Also referred to as "input image."

Real-time facial recognition involves facial recognition algorithms that can be used while a video recording is taking place and the process of capturing the biometric data, comparison, and identification are all done instantaneously.

Similarity score - score assigned based on the probability that the returned image is a match for the target image.

Target photos - photographs that are returned based on the parameters of the threshold, or similarity score to the probe photo or input image. Also referred to as "comparison photo" and "returned photo."

Threshold - any real number against which similarity scores are compared to produce a verification decision or gallery of images.

Example Law Enforcement FRT Policy *Appendix B: Acronyms*

An agency shall compile a list of appropriate acronyms that are relevant to that particular agency.