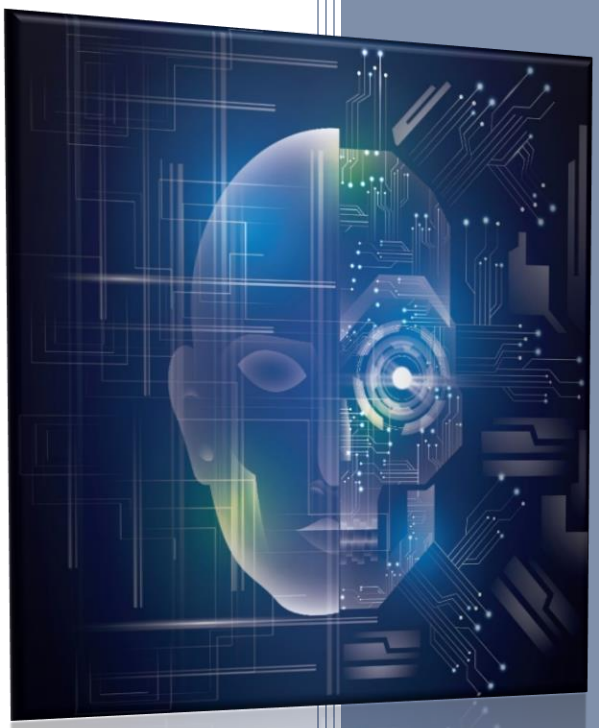
IJIS Institute

LAW ENFORCEMENT FACIAL RECOGNITION USE CASE CATALOG



Law Enforcement Imaging Technology Task Force

A joint effort of the IJIS Institute and the International Association of Chiefs of Police

February 2019

ACKNOWLEDGEMENTS

The IJIS Institute would like to thank the following IJIS Institute and International Association of Chiefs of Police (IACP) contributors as well as their sponsoring companies and organizations for supporting the creation of this document:

Contributors

- Patrick Doyle – LEITTF Co-Chair and New Jersey State Police, Lieutenant (Ret.)
- Bonnie Locke – LEITTF Co-Chair and Nlets Business Development Director
- Jamie Algatt – Senior Product Manager, RapidDeploy USA
- Steve Ambrosini – Program Director, IJIS Institute
- Ben Bawden – Partner, Brooks Bawden Moore LLC Consultants
- Maria Cardiellos – Director of Operations, IJIS Institute
- Robert E. Greeves – Senior Policy Advisor, National Criminal Justice Association
- Pete Fagan – Virginia State Police, Lieutenant (Ret.)
- Jenner Holden – Chief Information Security Officer, Axon
- Robert May – Program Director, IJIS Institute
- James Medford – USAF Lt. Col. (Ret.)
- Catherine Miller – National Capital Region NCR-LInX Program Manager
- Dave Russell – Director, Northern Virginia Regional Identification System
- Pam Scanlon – IACP CJIS Committee Chair and Director, ARJIS/San Diego
- David M. Shipley – Executive Director, Colorado Information Sharing Consortium
- Robert Turner – President, CommSys Incorporated
- Gerald L. Ward, Ph.D. – MTG Management Consultants, LLC
- Heather Whitton – Cincinnati Police License Plate Reader Program Manager

EXECUTIVE SUMMARY

This Law Enforcement Facial Recognition Use Case Catalog is a joint effort by a Task Force comprised of IJIS Institute and International Association of Chiefs of Police members. The document includes a brief description of how facial recognition works, followed by a short explanation of typical system use parameters. The main body of the catalog contains descriptions and examples of known law enforcement facial recognition use cases. A conclusion section completes this catalog, including four recommended actions for law enforcement leaders.

TABLE OF CONTENTS

FOREWARD

Police work is constantly adapting to an ever-changing environment, yet it has always been grounded in one simple, founding principle – to make the world a safer place.

To that end, law enforcement agencies, and other public safety entities must not only stay abreast of the latest tactics and technologies used by criminals, but also deploy every available method to maintain order, thwart wrongdoing, and ensure that those who threaten the peace are held accountable for their actions – all while respecting the Constitutional rights of those involved.

However, new police technologies and procedures do not automatically coincide with new laws, rules, or policies governing their use. Their initial deployment can sometimes be misunderstood, and, in some cases, technological capabilities in the hands of law enforcement can exceed the public's comfort level. It can take some time before both citizens and the courts widely accept high-tech police tools. Such a learning curve and adjustment period has occurred with everything from issuance of police firearms to traffic radar speed monitoring devices.

What is unknown is often feared – or at least misunderstood – sometimes leading to overreactions and overreaching by policy makers. This response can limit the extraordinary new ways these amazing advances can help ensure public safety.

Today we are wrestling with similar issues in the case of facial recognition, which is sometimes referred to as facial analysis or face matching. Facial recognition is a remarkable development that helps law enforcement exonerate the innocent, narrow searches for the guilty, and otherwise maximize limited resources. Simply put, it greatly expedites certain police functions through the rapid comparison of one facial image to many others.

While the term *facial recognition* has become somewhat synonymous in the media and among other stakeholder groups to describe all uses of this technology, such systems used by law enforcement actually provide recognition of *potential* candidates, not recognition of *exact* matches as the name might insinuate. Law enforcement best practices for all known use cases still requires a human examiner to confirm that one of the computer-provided candidates actually matches the submitted image. The computer or software system does not make the final decision regarding an exact match when proper police procedures are being followed – a trained person does.

Public safety professionals use facial recognition in various ways to help them discover or find individuals, and to assist with the identification of people. But, because facial recognition uses the very personal and particular attributes within an image of the human face, it has a very private and individual connotation to it. The fact that it can help sort through great volumes of images, and that citizens aren't necessarily aware their own faces are in such comparative databases, only heighten the potential anxiety over the use of facial recognition technologies. These issues, combined with the tendency of police to adopt successful measures quickly to protect the public *prior* to enacting fully vetted policies, have created an environment where something as promising as facial recognition has the potential to be viewed as a problem itself, rather than an answer to one.

What appears to be immediately needed is a balanced and well-informed approach to facial recognition by authorities, which will help ensure public understanding of the way in which the technology is used by law enforcement, and to what end.

PURPOSE OF THIS CATALOG

The IJIS Institute and the International Association of Chiefs of Police (IACP) are both research entities and policy advocacy bodies, but each has different core memberships. The combination of these two groups into a task force provides a multi-faceted perspective to technology issues. IJIS is a nonprofit alliance of industry leaders, technology developers, practitioners, national associations, and academic organizations, while IACP is comprised largely of justice leaders, law enforcement practitioners, and police vendors. The blend of experience and competencies between these organizations is a desired benefit in this catalog.

With a combined membership of more than 30,000 global representatives, IJIS and IACP together have deep knowledge, academic prowess, and practical experience to wrap their arms around emerging issues and technologies. The organizations have created a joint research effort known as the Law Enforcement Imaging Technology Task Force (LEITTF) to review emerging trends and technologies such as facial recognition.

The LEITTF has created this document as a catalog of facial recognition use cases for criminal justice agencies, which includes uses by police officers, sheriff's deputies, investigators, and supporting personnel wherever they exist. This examination of uses covers typical settings wherever law enforcement interacts with persons such as large venues, transportation hubs, correctional facilities, motor vehicle stops, crime scenes, and other everyday situations.

The intention of this effort is to briefly describe facial recognition systems and their parameters, determine the ways in which facial recognition is being used, and, most importantly, to document cases which demonstrate the technology's ability to protect the public. The objective is to empower public safety practitioners and industry innovators to communicate the ability of facial recognition to policy makers and the public, while reducing misunderstanding and minimizing the potential misuse.

The LEITTF has chosen to catalog and explain facial recognition use cases (as opposed to creating model policy, conducting a scientific analysis, or examining other elements of facial recognition) in order to fulfill an immediate need to improve visibility into how these systems are used. Providing real examples from the field further strengthens the context of facial recognition usage so that those outside of law enforcement can appreciate its necessity. It is hoped such details will help encourage outreach from police to concerned citizen groups and, in general, establish a better understanding of facial recognition. Describing the way in which facial recognition is successfully deployed should increase awareness and alleviate at least some of the public's concerns, and also perhaps spur healthy discussion into areas where citizen apprehension persists. As has been proven with every successful deployment of technology and

law enforcement effort to combat crime, "you cannot police a community without effectively working with that community."[1]

HOW DOES FACIAL RECOGNITION WORK?

Facial recognition has been in limited use for many years. Recent improvements in system accuracy combined with higher demands for biometric identification capabilities have led to more widespread use in private industry such as corporate settings, with public and law enforcement use lagging slightly behind but certainly on the rise.

A typical facial recognition system uses the layout of a subject's facial features, and their relative distance from one another, for identification comparison against a separate image, or perhaps even against thousands or even millions of separate images in a database or gallery of faces. The subject's facial image attributes are derived from either a still or video image – physical presence is not always required.

Computer algorithms then measure the differences between the face being searched and the enrolled faces in a chosen gallery, such as a government database of images. The smaller the differences between the faces considered, the more likely those faces will be recognized and presented as potential matches. Through statistical analysis of the differences, a facial recognition system can provide a list of candidates from the gallery and rate the most likely matches to the image of the subject's face. Using generally accepted law enforcement best practices, a trained face examiner would then make the final selection, potentially determining one of the candidates is very likely a match to the original submission. Of course, some facial recognition searches result in no high-probability match candidates. Even if the computer algorithm does return potential match candidates, it is possible, and, in fact, common, that the trained human examiner does not agree, nor does he or she select any candidate as a likely match.

Perhaps the most important element regarding the use of facial recognition by law enforcement is not within the technology itself, but what follows once the computer has suggested candidates and the human examiner determines a likely match exists in a particular case. It is at this point that the police have a strong clue, and nothing more, which must then be corroborated against other facts and investigative findings before a person can be determined to be the subject whose identity is being sought. Therefore, a candidate match, even after confirmation by a trained user, is, in most jurisdictions, not enough evidence for police to detain or arrest a person. All facts, and the totality of circumstances regarding the investigation or search, should be considered before any action is taken.

[1] William Bratton, former NYPD and Boston Police Commissioner, and LAPD Chief.

Facial Recognition Use Types

Facial recognition technology is broadly used in two different sorts of law enforcement situations:

Identify	It can help **identify** a subject face against a known image. For example, this would help confirm that a face presented at a border checkpoint may be a match to the digital image of a face embedded in a document, such as a passport. This is sometimes known as **one-to-one analysis**, since facial recognition is being asked to provide guidance on whether one submitted sample image is likely the same person as in another image. 
Discovery	Facial recognition technology can also help compare the image of a face to a number of known faces within an array or database. For example, this helps police use technology to suggest if a criminal or terrorist in a surveillance video or still image may match any mug shot photos of people previously arrested or convicted. This function is typically called **discovery** and is sometimes referred to as a **one-to-many analysis** since it seeks to compare one image to multiple other images to find candidates for potential matching. 

Facial Recognition System Parameters

There are several elements of a facial recognition system which are somewhat similar to other database-reliant technologies. For instance, digital fingerprint systems retain a repository of collected prints, and in many cases, newly submitted prints are often compared to those in the database to see if there are potential prints which may match the sample. It is also possible to compare one set of collected prints to another collected set or print, such as from a crime scene. Facial recognition is often used in similar ways – comparing one-to-one, or comparing-one-to-many. However, there are several distinct differences since facial recognition is currently somewhat unregulated by laws, policies, and practices regarding image capture, usage, retention, accuracy, and human oversight.

Also, face images can be collected much more easily than fingerprints, sometimes without the person knowing an image of their face has been captured. Most people that are fingerprinted have either consented to prints being taken or have been arrested and have no choice. Face images are sometimes collected with consent, such as with a driver's license photo, but an extended or implied consent over its future use in a repository is not usually given. In some cases, governments prohibit implied consent or do not allow the agency capturing the original photo to even ask for it.

However, in some regions, consent to capture the photo for one purpose does not always expressly prohibit its use by law enforcement. Therefore, some police agencies may use captured images without a person's expressed consent, but not necessarily against their wishes.

These types of image captures, uses, and retentions, and the fact that there are no consistent laws or rules throughout many states, provinces, territories, and countries, have helped cause misunderstandings and some resistance to facial recognition systems.

Facial recognition accuracy is also an unsettled discussion in many regions. This technology is without question much more efficient at scanning through large numbers of photos to find potential candidates which are very similar to the submitted image, but there are questions about whether or not it can ever be 100% accurate.

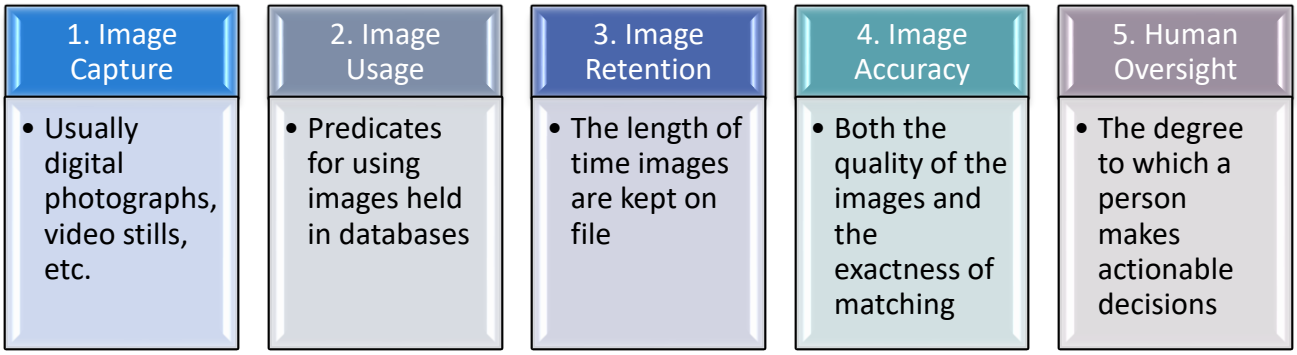
Some facial recognition research, such as the Georgetown Center for Privacy and Technology Report,[2] have widened the gap between supporters and detractors through suggestions that the systems are at least partially biased toward minorities, and because of such inherent risks, should only be used by police to find very serious criminals. Other recent studies, such as the latest reports by Massachusetts Institute of Technology's (MIT) Computer Science and Artificial Intelligence Lab[3] and IBM,[4] each suggest facial recognition bias can be mitigated through improvements in algorithmic structure, more racially inclusive data sets, and broader facial data point collection. Greater overall independent study is needed, and transparency regarding the results will be essential to maintain public confidence in the technology as the science is refined and fear is mitigated.

There are also media and watchdog group assertions that the technology is in some cases being used to single out a person based *only* upon a computer-driven algorithm's decision, without any significant amount of human oversight to the process. Many of these anecdotal complaints involve use cases where denial of entry or services is the result, such as admission to a sports stadium, *not* detention, arrest or formal criminal prosecution. However, any decision by law enforcement personnel which is made solely by software, no matter how inconsequential the decision may be, is alarming to some stakeholder groups. This type of facial recognition system usage certainly has stirred criticism, which is inadvertently fueled through accuracy improvements made by technology providers. Greater accuracy may cause some users of facial recognition, including law enforcement agencies, to rely more on the computer results than on human examiner decisions. However, police agencies should be held responsible for ensuring facial recognition systems are supported by strong policy, training standards, and human oversight, regardless of increasing accuracy, especially when criminal investigations are being conducted or other impactful actions may be taken which affect the public.

[2] Georgetown Law School Center for Privacy and Technology Report, *The Perpetual Line-Up*, October 2016 https://www.perpetuallineup.org/.
[3] Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory Study, *Uncovering and Mitigating Algorithmic Bias Through Learned Latent Structure*, January 2019, http://www.aies-conference.com/wp-content/papers/main/AIES-19_paper_220.pdf.
[4] IBM Corporation, *Diversity in Faces Study*, January 2019, https://www.ibm.com/blogs/research/2019/01/diversity-in-faces/.

Aspects of Facial Recognition System Deployments

Facial recognition system deployments generally have five significant aspects:



These five aspects each have important variables, leading to potentially different best practices, policies, laws, limitations, and concerns depending on the exact use cases.

Here are the five system aspects listed again, with potential questions concerning usage parameters following each:

Image Capture	Who captured the image? When was it captured? How was it captured? Why was it captured? Was consent given to capture it?
Image Usage	Who will use the image? When will it be used? How will it be used? Why will it be used? Will consent be given each time it is used?
Image Retention	Who has the right to retain the image? When do they have the right to retain it? How will it be retained? For how long will it be retained?
Image Accuracy	Are image quality, capture, and comparison methods standardized? Are both sample and gallery images similarly standardized? Are accuracy errors random or patterned by sex, race, skin color, affliction, style choices, image accuracy, etc.?
Human Oversight	Are trained examiners the ultimate decision makers? Are examiners trained to certain standards? How often?

Some of these questions may each be answered differently, depending on how facial recognition is being used at the moment, and under what pretenses, and by which type of agency. That is why this catalog presents the following actual known law enforcement use cases of facial recognition systems. These use cases should provide context as to why the public's opinion of this technology may be quite different depending on the actual circumstances of its use and may further depend on the timing of such police use within the justice continuum. What is publicly acceptable for law enforcement to use when detaining known criminals or investigating crimes may not be tolerable for those situations where police are conducting broad surveillance, or routinely patrolling neighborhoods. Examination of law enforcement facial recognition uses cases may help both the police and the public come to terms with how this technology is, and should be, deployed.

USE CASES

Police officers are generally very adaptive and ingenious, probably because their profession calls for it, and their own survival often depends on it. The nature of protecting the public usually requires quick-thinking, and the use of things which may go beyond their original intended design is sometimes a necessity.

Such is the case with facial recognition, which was originally intended as a fairly specific investigative tool to help narrow the field of suspects down to a manageable amount. However, law enforcement professionals quickly learned to deploy it as a means of exonerating the falsely accused, identifying the mentally ill, helping return children to their parents, and determining the identity of deceased persons, in addition to other innovative uses.

This Task Force found at least 19 known uses of facial recognition for law enforcement. These uses involve both overt, and covert, facial image capture and observation techniques.

Law Enforcement Facial Recognition Use Case Categories

The different ways in which this technology is being used generally fit into three different groupings, based upon the activity or required tasks of the law enforcement professional using facial recognition:

1. Field Use
2. Investigative Use
3. Custodial and Supervisory Use

Many of the 19 uses can also be performed with two distinctly different intentions:

- **Discovery** – helping to find one person among many persons *(One-to-Many Comparison)*
- **Identification** – helping to verify one person is in fact the person being helped or sought *(One-to-One Comparison)*

The database of comparative photos use in each use case can also differ. For example, some law enforcement agencies may use images from public sources (such as department of corrections records) to compare with a recently captured image of a suspect. Other police departments may also use a privately-owned gallery, such as one maintained by a sports venue security firm, which, for example, may have been created from video surveillance or ticket-use photo identification databases.

Therefore, each use case may have several variables, such as the intended outcome to either *discover* a person, or *identify* a person, plus be conducted using comparison to either public and private sources of photos, or both, and at different points in an investigation or inquiry into a matter brought to the attention of police, Figure 1.

Figure 1

In the following use case descriptions, actual instances or example scenarios follow each use case to further clarify the ways in which facial recognition may be used by law enforcement.

Field Use

The following situations generally occur where an officer uses facial recognition to help positively identify an individual during a face-to-face interaction, or during some other active, uniformed-police response to an incident.

Random Field Interaction

An officer on patrol in the field may be alerted that an individual's image actively captured on an operating in-car or body worn camera may be a possible candidate for a match to a subject in a wanted persons image database.

Example Scenario

Police officers assigned to foot patrol in a business district may be required to operate their body worn cameras during all substantive interactions with the public. During such patrol duties they are often approached by citizens with questions, comments, or complaints, at which time face images captured via activated body worn camera footage may be compared in near real time to a criminal warrants database of fugitive images.

Reasonable Suspicion Interaction

An officer may be alerted to unusual or furtive activity by a person, which presents reasonable suspicion to capture an image of the individual to protect the officer's safety, or to potentially explain the suspicious activity.

Actual Instance - Fugitive Apprehended

In January 2017, an officer assigned to a fugitive task force observed a transient male that matched the description of a known wanted subject. The male was uncooperative and refused to identify himself. The officer captured a photograph of the subject and used facial recognition as one tool to help identify him. The officer then queried NCIC and was informed that the subject had an active felony warrant. He was booked and the case was closed.[5]

Active Incident

During an active criminal situation, video or pictures obtained by officers could be used to potentially help identify individuals and guide active response efforts.

Example Scenario

A situation might occur where a field officer records video of a person's face, such as with an in-car or body worn camera system, and the person then flees the scene of the encounter. Facial recognition could be used to compare the recorded image of the person's face against a database to help determine who the person might be, or why they fled.

Deceased Identification

Deceased individuals can be more quickly identified in the field with facial recognition systems providing possible matched images to a captured imaged of the victim.

Actual Instance - Facial Recognition Used to ID murder victim

Police received a 9-1-1 call of a male subject lying in the street. Officers arrived and located an obviously deceased adult male victim in the roadway. There was evidence of trauma to the victim's body and it would eventually be learned that a homicide had occurred. The victim did not appear to possess any identification and responding detectives were initially unable to identify the subject. A photograph was taken at the crime scene and submitted through a facial recognition program. Within minutes, a candidate photograph was returned, helping to identify the victim as 21-year-old male. This identification was corroborated by other facts obtained in the early stages of the investigation. The speedy identification of the unknown victim in this case was a huge benefit, making it possible for timely notification to the family, and moving the investigation forward towards its eventual resolution through the arrest of two suspects.[6]

[5]Automated Regional Justice Information System, San Diego, California.
[6]Automated Regional Justice Information System, San Diego, California.

Lost & Missing

Lost children or missing adults could be located and identified when encountered by officers during interactions, whereby facial recognition is used to help provide clues to determine identity.

Example Scenario

A situation might occur where a field officer encounters a lost child or disoriented adult and captures an image of the person's face for comparison with a database of lost or missing persons to help identify them.

Interdiction

An individual of interest who is actively avoiding identification can potentially be located at a checkpoint, with facial recognition providing clues for officers to investigate.

Actual Instance - Illegal Alien Attempts Entry

In August 2018, a 26-year-old man traveling from Brazil entered Washington Dulles International Airport and presented agents with a French passport. Agents used facial recognition to compare his passport photo to a database of known images with identities and were alerted that the man's photo might not be a match to his stated identity. The man became nervous when agents referred him for a secondary search. The agents discovered the man's real identification card in his shoe, and it was revealed he hailed from the Republic of Congo. Charges are pending.[7]

Identify Fraud

Incidents often occur where a person presents identification documents to fraudulently obtain access or services, such as voter, benefits, or border access privileges, and facial recognition can be used to alert officers to possible mismatches.

Actual Instance - Credit Card Fraud

An unknown female pictured in surveillance photos entered a costume store attempting to purchase multiple wigs with a credit card that was stolen from a vehicle earlier in the day. The transactions could not be completed as the cardholder had already canceled the stolen cards. At this time, it is unknown whether the pictured female was also involved in the vehicle trespass. The female was described as having a heavier-set build and dark, shoulder length hair. Checking the surveillance photos against a correctional mug shot database with the agency's facial recognition application revealed the identity of a high-probability candidate, who is now under investigation for use of the stolen credit card.[8]

Actual Instance – Retail Fraud

On March 5, 2018, investigators opened a case involving fraud and the use of counterfeit traveler's checks ranging from $5,000 to $20,000 in multiple jurisdictions. A male and female

[7]United States Customs and Border Protection.
[8]Arapahoe County, Colorado Sheriff's Department.

suspect had opened a membership at a Costco and began using the checks as payment. The investigating agency submitted the new member photos to a facial recognition application and investigators were able to locate candidates in the system and eventually confirm the identities of both suspects. Charges are pending.[9]

Actual Instance - Retail Fraud and Theft

Around April 13, 2018, investigators received an Asset Protection Alert from a local Home Depot not in their jurisdiction. The suspects in these cases have stolen over $5,000.00 in tools from Home Depot stores in nine separate cases and five different stores. The investigator used the agency facial recognition application to compare surveillance photos of the suspect with photos from a correctional mug shot database. The application returned a high-probability candidate now under investigation by Home Depot retail crime investigators and local authorities. Charges are pending.[10]

Actual Instance - Retail Fraud

On June 20, 2018, investigators received a bulletin advising that a suspect has committed two high-dollar thefts at The Home Depot. The suspect was targeting Milwaukee power tools. Total loss for the two cases $1,097.00. Surveillance photographs were entered into the agency's facial recognition application used to search the correctional mug shot database. The application identified two high-probability candidates that additional investigation confirmed were the involved suspects and resulted in recovery of the stolen tools and pending charges.[11]

Investigative

The following use cases generally involve law enforcement using facial recognition technologies to assist in solving crimes, such as use to gather evidence or aid in investigations.

Active Incident

During an active criminal situation, surveillance video can be used to provide images of suspicious persons which may help to identify suspects or witnesses, thereby guiding active response efforts.

Example Scenario

A situation might occur where a terrorist attack is made, and surveillance video of the area prior to the event is obtained. Images of suspicious persons in the video can be entered into other monitoring systems, which can then search for potential matches among other video feeds.

[9]Arapahoe County, Colorado Sheriff's Department.
[10]Arapahoe County, Colorado Sheriff's Department.
[11]Arapahoe County, Colorado Sheriff's Department.

Photo Array Construction

The creation of photo arrays can be automated using an existing suspect photo along with other biometrics information to find similar photos, thereby creating a photo array to be shown to a witness or victim for suspect identification.

Actual Instance - Armed Robbery Suspect Apprehended

An Indiana detective used facial recognition software to help identify a convicted serial robber as the alleged stickup man of a payday loan business. The business' cashiers told police the suspect ran around the counter and flashed a firearm before ordering them to empty two cash registers. Records show that the suspect ordered a cashier to open the store's safe but fled after he noticed a customer walking out of the business on her cellphone. The suspect's face was visible on the store's surveillance footage. Police released footage of the suspect the week after the robbery, but no leads were developed.

A detective then turned to the department's facial recognition software and put a photo of the suspect from the surveillance footage into the system which came up as a possible match. The detective showed the cashiers a photo array, which included the suspect's photo, and they identified him as the robber. The suspect had absconded from parole earlier this year in Illinois after serving part of a 12-year prison sentence for a string of armed robberies in the northwest Chicago suburbs, according to Illinois Department of Corrections records. He had committed nine robberies over the course of the prior 7 years.[12]

Actual Instance - Sexual Assault Suspect Apprehended

A 15-year old girl was sexually assaulted by an adult male she met online. The girl was only able to provide suspect personal information from his online profile but had also obviously met him in person, so she was familiar with what he looked like in real life and had access to online images of him. Police were able to use facial recognition on one of the digital images, which when compared to DMV photos, provided some candidates from which the girl was able to select a match. Authorities obtained a search warrant for the home of the identified suspect, who later admitted to the crime.[13]

Evidence Compilation

Photos of a known suspect can be used to search across existing traditional photo databases, or even situation-specific databases created from voluntary submissions, surveillance videos, or social media, yielding possible candidates which may match the suspect.

Actual Instance – Jewelry Thief Apprehended Via CrimeStoppers Comparison

On November 3, 2017, an unknown subject was caught on surveillance video at a Jeweler store, taking control over eight gold rings worth $2,000. The Hamilton County Sheriff's Office was asked to assist with the investigation and was in the process of testing its new facial recognition system. Deputies decided to use the jewelry investigation request as a training exercise. They used publicly-submitted CrimeStoppers photos to learn how to analyze the jewelry suspect image

[12]Munster, Indiana Police Department.
[13]Scranton, Pennsylvania Police Department.

to a candidate pool of images and were surprised that after just a dozen or so photos were compared, a strong candidate for a match was found. Detectives took this legitimate lead and started working with investigators from the original jurisdiction where the CrimeStoppers submission was made, piecing together the true identity of the suspect. The thief's identity was determined, and he was located and arrested for the jewelry theft, the CrimeStoppers Case and four other outstanding felony warrants.[14]

Actual Instance - Social Media Photo Helps Identify Suspect

A woman had an unfortunate encounter with a stranger whom she met on a dating website. The perpetrator's name and other personal information on his social network page were intentionally deceptive, but the photograph was genuine because his intent was to eventually meet the victim in person. Biometric search of the dating website profile photograph produced a possible match, which after further investigation, led to an arrest.[15]

Actual Instance - Suspect Misidentifies Sex to Avoid Arrest

A police officer used a facial recognition application to help identify a girl who was pretending to be a guy (Justin) instead of a female (Jamie), all to avoid being arrested on a warrant. No record came up on names and DOBs. Field officers used the available facial recognition application by snapping a photo of her in disguise and comparing it to the 4+ million booking photographs in the system. The suspect's FEMALE photograph returned as the #3 candidate. Immediate action on the returned information exposed the disguise and resulted in an arrest.[16]

Actual Instance - Shooting Suspect Apprehended

On October 17, 2018, a suspect identified by a witness as a tattoo artist and recently-released inmate, known only by the monikers Dough Boy *or* Dough Blow*, shot and seriously injured another person. Using information developed through a bulletin and photos from social media posts made by the suspect, the agency facial recognition application returned a high-probability candidate from a mug shot database. Further investigation revealed a high-probability candidate that the continuing investigation confirmed as the suspect in the shooting. The investigation continues.*[17]

Participant Party Identification

Facial recognition can be used to help confirm a witness, victim, or participant was at a specific crime scene, or associates with a specific suspect or group.

Actual Instance - Biometric Segmentation Helps Support Arrest

The CCTV imagery retrieved from a crime scene contained the face of the perpetrator. However, the quality of the images was too low to allow accurate unrestricted search against the entire image database. The face examiner used her crime analytics expertise to restrict the biometric search primarily, though not exclusively, to the criminals of a particular race, gender, age group, prior charges, and even the location of prior bookings. The search produced two leads

[14] Springfield Twp. Police and Hamilton County Sheriff's Office, Ohio.
[15] Safran MorphoTrust Corporation.
[16] Lakewood, Colorado Police Department/Colorado Information Sharing Consortium.
[17] Denver, Colorado Police Department.

which were further investigated by detectives in the field, with one of the leads leading to arrest.[18]

Victims Identification

Facial recognition can assist in potentially identifying victims of crimes, in situations where traditional methods of identification are not available.

Example Scenario

A situation might occur where a victim of a crime appears in a videotape or photograph, such as with a teenager being used in sexually explicit materials, but no report of crime is made to police by the victim or his/her guardians. The image of the victim can be used to search available databases for potentials candidates to be identified.

Criminal Identification

During the monitoring of large gathering places, transit locations, public property or areas of regular criminal activity, images of repeat offenders or known wanted persons can be compared against video images to help locate potential matches.

Example Scenario

A situation might occur where a defiant trespasser or registered sex offender is not allowed on certain public properties, such as playgrounds or schools, because of prior criminal convictions. Facial recognition could be used to monitor surveillance video for potential candidates who might match the identity of the prohibited person.

Suspect or Associate Identification

Facial recognition can be used to acquire images and potentially help identify existing or new subjects of investigations.

Actual Instance - Smart Phone Digital Photo Comparison Exonerates Suspect

A witness in a gang-related assault case provided smartphone photos of the suspects to the detective working the case. One of the photos of an unknown suspect was able to be run against facial recognition software and an investigative lead was developed. Upon further investigation confirmation of the suspect's name was made and during the investigation it was found that the suspect was in jail in another location. Verification of the suspect was made based on the photo and the photos of the tattoos on his arm. Apparently, the witness provided an incorrect photo of one of the suspects and the facial recognition system along with further investigation saved investigators time, and more importantly, saved the individual from being arrested for a case in which he was not involved.[19]

[18] Safran MorphoTrust Corporation.
[19] United States National Capital Region Facial Analysis Pilot Test Project.

Actual Instance - Homicide Suspect Identified

In April of 2018, Edgewater, Colorado, Police had a shooting death resulting from an attempted random street robbery and at the onset of the investigation had no suspect information or leads. From leads that were eventually put together, police were able to identify a suspect vehicle which was impounded. A receipt to a 7-Eleven was found in the vehicle and grainy footage from the store video system was obtained showing the suspects inside the store approximately one hour after the homicide. Three of the four parties seen in the video were identified by traditional means and subsequently arrested.

A fourth suspect/witness was seen but detectives were unable to identify her. With Wheat Ridge Police help, detectives used a facial recognition program to help identify and locate this female. This person ended up being in the car at the time of the homicide and was able to tell us exactly what happened the night of the homicide, who pulled the trigger and what other roles other people inside the vehicle played.

During subsequent follow up, the suspects made incriminating statements to multiple people on Facebook about the homicide. Detectives used the facial recognition program to help identify pictures of people found on their Facebook profiles since nobody uses their real name.[20]

Actual Instance - Theft Case Solved

An investigator had a theft case where the victim met the suspect for a date. When she went to the restroom, he stole her wallet. The only thing she knew about him was his first name. She had downloaded a picture of him on her phone. The agency's facial recognition application and the statewide mug shot database, identified a high-probability candidate, returning both identity information and extensive arrest information. The detective used the application's photo lineup feature, showed it to the victim and she recognized the identified candidate immediately. Charges are pending.[21]

Actual Instance - Carjacking Suspects Found

Two men attempted a robbery of a woman in the parking lot of a liquor store. The woman bravely fought off attempts to have her wallet and car taken, and the men fled. The store owner provided surveillance video of one of the men, who had entered the store to make a small purchase while stalking the victim. The video provided an image of the suspect, which was compared to a correctional photo database, revealing potential suspect candidates. Further investigation led to the apprehension of both the man in the video and his accomplice brother.[22]

Custodial & Supervisory

The following use cases use facial recognition technologies to potentially identify and track candidates as part of efficiently operating criminal justice system programs.

[20] Edgewater, Colorado Police Department.
[21] Arapahoe County, Colorado Sheriff's Department.
[22] Greenville County, South Carolina Sheriff's Department.

Admittance Identification

Facial recognition can be used to help authenticate the identity of arrested persons being booked into detention.

Example Scenario

A person arrested by a police officer for a crime might refuse to identify themselves. The suspect is often brought to a correctional facility. Booking officers usually obtain a photo upon processing, thereby comparing it to existing photos on file to potentially positively identify the suspect.

Access Control & Movement

Identity verification of inmates or other persons can be aided via facial recognition, helping to control access to certain areas of a detention facility, or assist in confirming identity before receiving medication, privileges, or access to items restricted to other inmates.

Example Scenario

A correctional facility controls access to certain privileged areas and needs to ensure inmates required to present themselves for certain actions are properly identified. Officers can use facial recognition to corroborate with other means of identification, such as ID bracelets, RFID devices, and other biometric indicators.

Identification for Release

Confirming an inmate's identity prior to approved temporary or permanent release can be aided by facial recognition.

Example Scenario

A correctional institution obviously needs to control egress from its facility. Facial recognition can be used to help ensure an inmate presenting him or herself for work furlough, or release at the end of their sentence, is in fact the prisoner which should be allowed to leave the facility.

Identification for Program Participation

Facial recognition can be used to help confirm identity for special program participation, such as parole, probation, or sex offender registry.

Example Scenario

A parole or probation officer may be required to positively identify a person presenting himself for a urine test or mandated parole check-in visit. Facial recognition may be used to help establish a positive identity in concert with other biometric systems or identification processes.

Court Appearances

Identification of a court defendant or witness can be further corroborated using facial recognition.

Example Scenario

A judge may order a defendant appearing before her positively identified, especially in cases of identity fraud, exact twins or undocumented aliens with no official government identification. Court officers could use facial recognition to assist in the positive identity of the person by comparing the person's face with available databases.

CONCLUSION

Facial recognition is a powerful and highly efficient tool which can significantly increase public safety. With such power, however, comes great responsibility.[23]

Maintaining public trust in law enforcement is an even greater calling than apprehending criminals, as one makes the other easier, and must always precede the latter. Technologies like facial recognition systems are essential to help police maintain order in the modern world but must never be deployed or used to the detriment of the good opinion citizens have for their protectors. A popular, yet sometimes forgotten, axiom states, "the police have authority because the public allows it," meaning without the goodwill of citizens, the job of law enforcement would be impossible. This concept is the basis for most democratic society policing principles, derived from law enforcement pioneers who thought it important to cultivate citizen support, as without it, "public opinion is a compound of folly, weakness, prejudice, wrong feeling, right feeling obstinacy, and newspaper paragraphs."[24]

Recommendation #1: Fully Inform the Public

Law enforcement should endeavor to completely engage in public dialogue regarding purpose-driven facial recognition use, including how it operates, when and how images are taken and retained, and the situations in which it is used.

With facial recognition systems, the most powerful aspect is its use to compare as many images as possible in a short amount of time. It helps automate a laborious manual process to aid in many public safety efforts. Therefore, maximizing lawful and accepted use of images should be paramount, and providing the public with confidence that such capture and comparison are done fairly will ultimately ensure the most successful use of facial recognition.

[23] This idiom is widely attributed to an unknown contributing author of the National Convention Decrees during the French Revolution, May 8, 1793

[24] Sir Robert Peel, British Statesman and founder of the London Metropolitan Police in 1829.

Recommendation #2: Establish Use Parameters

Appropriate system use conditions, even preliminary ones, must be established as soon as possible to engender public confidence it its use and avoid any further proliferation of mistrust.

The use cases within this document demonstrate the varied ways in which this one technology can be deployed into many aspects of public safety. No doubt more uses will arise over time, bringing facial recognition systems to bear against all manner of crime, and on behalf of many victims, just as fingerprinting and DNA matching have done in the past.

The real cases presented are but a small sampling of the thousands of success stories, many exonerating the wrongly accused as well as bringing the correct criminal to justice. It is hoped that more cases will be brought to light through enlightening discussions such as those this document attempts to create.

Recommendation #3: Publicize its Effectiveness

All public safety agencies should widely publish facial recognition success stories to heighten overall awareness of its usefulness, especially those cases in which suspects are exonerated, or where facial recognition is used to protect vulnerable persons.

This description of facial recognition systems and the ways in which it is being used by police is a starting point. While it is most often used to apprehend criminals, it is also used to find missing children, identify deceased persons and help prevent the innocent from being accused. Through consideration of the identified issues and these use cases, human reference points will be created so that the technology's interactions with citizens will be less mysterious and more appreciated for the service if provides. It is also hoped that by outlining how it is used throughout law enforcement, it will help stimulate needed conversation, policy creation and baseline training standards that can be tailored to each use within accepted community tolerances.

Recommendation #4: Create Best Practice Principles and Policies

Model law enforcement facial recognition guidance and regulation documents should be immediately established and broadly adopted, to include training benchmarks, privacy standards, human examiner requirements, and anti-bias safeguards.

Initial training and periodic re-training certifications are required as a part of most law enforcement technologies, and facial recognition seems to need such best practice standards to ensure both the courts and the public have a confidence in its consistent, fair use. Only after a broader public and judicial acceptance of facial recognition is created and stabilized can it then realize its full potential in becoming one of the most efficient and amazing law enforcement tools every deployed.

None of this catalog's representations, nor its recommendations will be constants – things change at a record pace these days, and so too must the ways in which we view and regulate ourselves as well as our machines. However, the use cases presented, and the suggestions within this report to improve the standing of facial recognition, should be immediately useful to help get this technology back on a positive trajectory.

The LEITTF believes strongly in facial recognition abilities and reasonable use conditions, and highly recommends enlisting the public more directly to generate wide support for our collective mission – to make the world a safer place.

RESOURCES

For more information about facial recognition technologies and opposition to it:

❖ IACP Technology Policy Framework	https://www.theiacp.org/sites/default/files/all/i-j/IACP%20Technology%20Policy%20Framework%20January%202014%20Final.pdf
❖ City of Palo Alto Surveillance Technology Ordinance	https://www.cityofpaloalto.org/civicax/filebank/documents/66597
❖ U.S. Bureau of Justice Assistance Policy Development Template	https://www.bja.gov/Publications/Face-Recognition-Policy-Development-Template-508-compliant.pdf
❖ Georgetown Center for Privacy & Technology Face Recognition Use Policy	https://www.perpetuallineup.org/appendix/model-police-use-policy
❖ Electronic Frontier Foundation Police Uses of Facial Recognition	https://www.eff.org/wp/law-enforcement-use-face-recognition

❖ Cardiff University Evaluation of Police Facial Recognition Use Cases	https://crimeandsecurity.org/feed/afr
❖ ACLU Report on Test Use of Facial Recognition at U.S. Capitol	https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28
❖ Michigan State University Case Study of Facial Recognition Use in Boston Bombing Investigation	http://biometrics.cse.msu.edu/Publications/Face/KlontzJain_CaseStudyUnconstrainedFacialRecognition_BostonMarathonBombimgSuspects.pdf
❖ Draft Model Police Facial Recognition Policy (James Medford, USAF Lt. Col. (Ret.)	https://drive.google.com/open?id=1BzKrSo-kLUV8uI88gwUm_1Du3ewePwVZ

REFERENCES

Georgetown University Law School Center for Privacy and Technology Report, *The Perpetual Line-Up*, October 2016, https://www.perpetuallineup.org/.

Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory Study, *Uncovering and Mitigating Algorithmic Bias Through Learned Latent Structure*, January 2019, http://www.aies-conference.com/wp-content/papers/main/AIES-19_paper_220.pdf.

IBM Corporation, *Diversity in Faces Study*, January 2019, https://www.ibm.com/blogs/research/2019/01/diversity-in-faces/.

ABOUT THE IJIS INSTITUTE

The IJIS Institute is a nonprofit alliance working to promote and enable technology in the public sector and expand the use of information to maximize safety, efficiency, and productivity.

The IJIS Institute has members and associates working within and across several major public-sector domains as our areas of focus:

- Criminal Justice (Law Enforcement, Corrections, Courts)
- Public Safety (Fire, EMS, Emergency Management)
- Homeland Security
- Health and Human Services
- Transportation

IJIS Institute is the only national membership organization that brings together the innovative thinking of the private sector and the practitioners, national practice associations, and academic organizations that are working to solve public sector information and technology challenges. IJIS Institute advocates for policies, processes, and information sharing standards that impact our safety and security, builds knowledge on behalf of our stakeholder groups, and connects the organizations and leaders within the communities of interest.

The IJIS Institute provides a trusted forum within and across our areas of focus where resources are developed, collaboration is encouraged, and public-sector stakeholders can realize the benefits of technology and the power of information to keep our communities safe, healthy, and thriving.

Founded in 2001 as a 501(c) (3) nonprofit corporation with a national headquarters in Ashburn, Virginia, the IJIS Institute has grown to nearly 400 member companies and individual associates from government, nonprofit, and educational institutions from across the United States.

The IJIS Institute thanks the Law Enforcement Imaging Technology Task Force for their work on this document. The IJIS Institute also thanks the many companies who have joined as Members that contribute to the work of the Institute and share in our mission to drive public-sector technology innovation and empower information sharing to promote safer and healthier communities. For more information on the IJIS Institute, visit our website at http://www.ijis.org/.

About the Law Enforcement Imaging Technology Task Force

The Law Enforcement Imaging Technology Task Force was formed in 2015 as a joint project of the IJIS Institute and the International Association of Chiefs of Police (IACP). This Task Force was created to study new imaging software, devices, and methods as a means of ensuring successful, principled, and sustainable use which is both supported by citizen and aligned with the ultimate mission – to improve public safety.