The Bill Blackwood
Law Enforcement Management Institute of Texas

Facial Recognition Software for Patrol

A Leadership White Paper
Submitted in Partial Fulfillment
Required for Graduation from the
Leadership Command College

By
Dylan R. Eckstrom

Arlington Police Department
Arlington, TX
February 2020

ABSTRACT

Facial recognition technology is currently not being utilized in an efficient manner. There are alternative and passive applications which include individual safety for officers. There is an ability to link or identify persons of interest in active criminal investigations. Known suspects with active warrants provides an officer with the ability to increase awareness from available photograph comparison. The comparison of photographs is already publicly available, but utilizing the database for runaways, missing persons, be on the lookout, and active warrants, significantly increases an officer's safety awareness. Law enforcement should utilize portable facial recognition technology in its daily application. Facial recognition technology is a way to make officers more accountable, flexible in application, and safer during public interactions. In the full application and implementation of a portable facial recognition system, there will be a significant increase in awareness. This increase can potentially minimize injuries based upon knowledge that would normally not be present during an average interaction. The available comparison photographs are public information and used currently to disseminate information to the public. There is a subset of photographs which are law enforcement sensitive, which can easily be separated through a different search database, which would not be available to the public. Facial recognition is not biology; it is a statistical probability based upon unique facial features (Taylor, 2017).

TABLE OF CONTENTS

INTRODUCTION

Facial recognition technology should be actively implemented with law enforcement applications. Technology advances at an exponential rate, and with this advancement, there are direct and immediate applications involving law enforcement. Recent developments in technology include commercially available facial recognition software. The purpose of facial recognition software is to provide a layer of security towards a personal device with the intent to limit access. Facial recognition has already been utilized with existing security camera footage in identifying suspects through social media accounts and driver's license photos. However, this technology is being used in a static environment after events have occurred. Law enforcement has an opportunity to maximize this type of technology in a dynamic environment to assist in patrol functions.

Law enforcement can adapt facial recognition software in mobile devices to assist in identifying individuals who have active warrants, persons of interest, mental health warrants, missing persons, and runaways. Activation alerts based upon the type or category of interest in safety can also be added. An activation alert can assist in providing an officer with immediate officer safety alerts regarding felony warrants or violent offenders based upon a match with the facial recognition software. Alerts can help an officer identify unknown suspects involved in criminal activity once an image of the offender has been obtained, but not yet identified. A different type of alert can be used to assist in the identification of mental health warrants, missing persons, and runaways.

The portable facial recognition software devices also act as an additional layer of protection for society and can maintain accountability for officers. As officers encounter the public in a variety of interactions through consensual contacts, suspicious person/place, reasonable suspicion, and probable cause, this technology will assist in proper identification of individuals who refuse to identify themselves. A positive alert through the facial recognition software can assist in elevating a consensual contact into reasonable suspicion, therefore increasing the authority a law enforcement officer has to continue investigating the contact. As officers receive crime alerts involving unknown offenders, officers conducting consensual contacts can have the ability to also rule out citizens through the contacts made by the facial recognition. This technology has the ability to increase safety against violent offenders while also searching for missing and endangered individuals. Matching persons of interest should be done in real time, and delays do not match the public's expectations for protection (Massola & Preiss, 2017). Law enforcement should incorporate facial recognition technology into daily patrol functions.

POSITION

Portable facial recognition software will strengthen contacts and legitimacy with the public. Holding law enforcement accountable is a requirement due to their arrest authority. The proposal of utilizing this technology not only will strengthen the contact authority of an officer, but simultaneously make the generic public safer. This technology makes the public safer by locating persons who are missing or endangered, potentially saving lives. This technology will allow law enforcement to identify potential felony suspects in a more passive environment. Making these alerts in a more low-key

type of investigation will allow an officer to better prepare for hostile contact. If an officer can choose the location or type of contact, the officer has the ability to request additional units to safely take a person of interest into custody versus making a rushed decision based upon a suspect's action. This allows the officer to be active as opposed to reactive, which minimizes potential injuries to all persons involved. As officers make casual or consensual contacts with the public, alerts will be able to justify further investigation, where the lack of information will not give authority or justification for continual contact (Falk, 2007).

There have been documented cases where facial recognition has located suspects who have created a new identity. The match was based upon a driver's license photo, which matched a mugshot with a different name. This technology located the suspect who was committing welfare fraud (Falk, 2007). The ability to passively identify persons of interest will have an immediate impact in the safety of the public. The technology gives an officer better justification for making a contact, in addition to continuing further contact. The application and ability of the facial recognition software has developed into a series of complex algorithms which allow utilization of partial photographs. The ability to take a photograph containing separate pictures and combining them to create a better complete package for comparison. There is software currently available which allows the ability to adjust light sources and angle of a photograph to then adjust the picture to a direct forward-looking photograph. This allows pictures which were once not reasonable options for comparisons to now be valuable potential identification resources. It is possible this technology can include a person of interest but can also exclude a person during law enforcement contact.

There are alternative uses to maximize the efficiency of the portable facial recognition software. The technology is a balanced approach of individuals freedom and the safety of the public. The databases which active enforcement would be generated from would be limited to the quantity of photographs and the clarity of the individuals face. Expanding the technology for civilian use can be an additional way to assist law enforcement with the growing level of expectations pressed upon the career field. Examples are to include runaways, silver alerts, a child is missing (ACIM), Amber alerts, and be on the lookout (BOLO). During investigations into any type of missing person investigation, the first 24 to 48 hours are considered the most critical in successful outcomes (Kepple, Epstein, & Grisham, 2014). The current facial recognition technology is being utilized with the U.S. Amber Alert system and border crossing locations (Falk, 2007).

Creating partnerships with stake holders is one very effective dynamic which creates trust within the community. Imagine the unification of private companies which encounter the public daily being able to identify active AMBER alerts and these same systems coordinating with Silver Alerts and Missing persons. Combining resources can greatly enhance the ability to effectively communicate with community stake holders. As an example, consider Walmart's surveillance system being linked to the missing person, runaway, or Amber Alert database. Individual businesses can also upload photographs of known theft suspects which can alert loss prevention in real time to notify law enforcement immediately for identification purposes. This would be able to communicate the information to loss prevention without the explicit knowledge of the unique event. Law enforcement should not use these private businesses to actively

locate active felony warrants without a clarification or consent of the business' knowledge. Active criminal warrants being shared with a facial recognition software should be significantly limited to a type of immediate knowledge of danger to the public or individual victim. The safety of the public is primary when this type of technology is actively implemented. We have the ability to create a safer society by targeting known violent offenders.

Implementation of portable facial recognition software increases officer safety. Officers can be alerted to potentially dangerous offenders in a quicker and more efficient manner once a facial recognition alert is obtained. People are not always paying attention and are not necessarily good at recognizing faces. Prison inmates have been mistakenly released due to aliases and the trading of personal information within the prison system. Actively cross referencing the parolee would be minimized by applying the facial recognition software prior to release (Falk, 2007). Creating situations where less human errors occur will enhance the safety of officers, which also include prison guards. The technology can be utilized to not only take offenders into custody but to also prevent releasing an incorrect offender back into society.

In most contact, law enforcement officers are behind the curve. The individuals we are speaking to have specific knowledge of their past, current actions, and intent. An officer must be constantly aware and when we are involved in a situation with less information than the offender, the offender has the upper hand. This technology can provide us the ability to obtain specific information in a faster and more efficient manner. This technology can increase an officer's awareness, therefore making the safety awareness occur faster. The same technology can also be used to assist in identity

confirmation by unique scars or tattoos. Individuals arrested have their tattoos photographed and documented. One can use this technology to photograph a tattoo which can also return to a percentage match to assist in identifying an individual. Being able to confirm identities is essential in law enforcement and additionally minimizes civil liabilities. This application of technology has already been used in live security feed environments to make a continual match on a suspect and follow them through a subway, in a dimly lit, high populated area. An agency can monitor by use of live security feed and provided physical updates to officers on the ground (Wolford, 2009). Officers can also have the technology on their person to assist in the match of a person of interest, once the individual is located. This technology can be applied to current devices like body worn cameras.

COUNTER ARGUMENTS

The immediate concern by any governmental application of technology is an abuse of authority and the intrusion into the private lives of the individual. Any new addition to technology creates a new opportunity for abuse or misapplication. Facial recognition software being abused by law enforcement is a concern when individual liberties of citizens feel like they are being infringed. There is a concern involving an increase in false positives against minorities. The accuracy of the facial recognition technology still has its limitations and could potentially lead to false arrests. The cost of any new technology is potentially cost prohibited.

There is no right to privacy while any person is in an area considered open to the public. The government is limited by the constitution and the people have an inherent right of privacy. This technology is commercially available to not only public, but also to

private industries. A person does not have a right to privacy while occupying a public space. If a law enforcement officer is lawfully present, even on private property, a “plain view search” is considered reasonable. Similar concerns of the invasion of privacy have been linked to the license plate readers (LPR), but this type of technology is not only used for law enforcement purposes but also wrecker drivers. The application for wrecker drivers includes the ability to locate a vehicle which needs to be repossessed, and this can also alert to stolen vehicles. These activations of the LPR are always conducted from a fixed object on a motor vehicle being operated in a public space. Any available license plate in view of the public is not considered an illegal search. An LPR is attached to a patrol vehicle and passively reads license plates and alerts the officer to any potential match regarding warrants or stolen hits. Contained within the same application of the LPR reader, the same authority is reasonably granted to facial recognition software due to the lawful presence of a police officer or any type of enforcement conducted in the open public space. The active implementation of portable facial recognition technological device is no different. A match with the facial recognition software does not constitute the authority to arrest, but simply provides the officer the ability to continue contact based upon a reasonable suspicion.

The facial recognition match does not rise to a probable cause threshold, which allows the officer to arrest. The facial recognition match would provide a reasonable suspicion contact and can be utilized to create, in addition to other extenuating circumstances can eventually lead up to enough probable cause to arrest. Once a statistical match is identified, additional investigation is required. The utilization of the facial recognition simply informs the authority to conduct further inquiries (Falk, 2007).

The concept is very similar to a license plate reader (LPR). The concerns increase with the availability of private corporations or entities assisting the government with locating individuals using this type of facial recognition technology. The actual application of the facial recognition software is equivalent to a group of individuals who are referred to as super-recognizers. During the facial recognition process, there is a statistical score associated with each potential match (Falk, 2007). There are some individuals who are referred to as 'super-recognizers' who possess abilities which are equivalent to the facial recognition technology. The average number of super-recognizers have been estimated to be about 1 in 100 people (Gaidos, 2013). The introduction and utilization of the facial recognition software simply places the other 99 individuals on the same level playing field as a super-recognizer. Police super-recognizers displayed a 20% difference compared to the control group in identifying a lookalike test (Robertson, 2016). Technology has advanced to display an incredible accuracy within 1% depletion of a match to photographs when compared to photos being five years apart (Sofge, 2013). Since facial recognition is not considered probable cause for an arrest, "Facial recognition … cannot be deemed as absolute, and all matches remain possible" (Rodriguez, 2016, p. or para. 1). It is important to remember the application of this technology is based upon a percentage match and not true positive identification. Facial recognition can be up to 85% accurate, which also means there are potentially 15% false positives (Gross, 2017). The percentage match can assist with the location of individuals but does not currently have the level of confirmation of probable cause to justify an arrest. In Florida, deputies have used this technology by taking photographs, then uploading the pictures in its database, which provides the closest 24 matches

(Weiss & Davis, 2005). This ability to provide numerous possible matches should be considered a safety feature minimizing the improper use of the technology. This technology can be used to enhance the investigation or provide an avenue of continuous investigation for a detective unit if possible.

An additional variation of concern is unintentional bias or minority discrimination. Studies have been conducted on age-bias, race-bias, and gender-bias; these concerns are often unintentional, and the people with such biases are unaware they are even occurring (Gier, Kreiner, & Lampinen, 2017). With the facial recognition technology this unintentional bias is essentially eliminated since there is a physical photograph for a comparison. A study was conducted with a 6.7% match; only 22 out of 330 individuals positively recognized an older female due to age bias (Gier et al., 2017). Potentially all these biases are eliminated by the picture comparison photograph. Using a facial recognition software eliminates most of the guesswork associated with descriptions provided. The incidental bias, which is not uniquely negative, can allow the person that is being searched for or looked for to walk right pass anybody based upon assumption of what the individual might look like. These assumptions also incorporate clothing choices and worn accessories. I would recommend a limited approach with any utilization of public-private partnerships and the application of criminal arrest warrants versus public safety concerns.

The original technology involves a potential increase in misidentifications involving darker skinned individuals. This increase rating to a possible tier 1 match was due to darker complexions and the technology's inability to identify more points of identification comparatively speaking to a lighter skin individual. The technology has

only increased in accuracy, and as previously stated, this is not justification to arrest. Any possible activation, like an LPR hit, requires the officer to conduct further investigation for confirmation. These concerns can occur also with limited light sources and the clarity of the recording device.

When applying this technology, the cost of implementation and software maintenance would need to be a significant consideration. The potential for minimizing law suits and the release of incorrect prisoners is a significant positive tradeoff for the funds a government possesses. The technological advances are becoming more frequent and cheaper as time continues based upon continual innovations from the private sector. Hopefully, in less than a decade this technology will be available and implemented through multiple different avenues within the law enforcement community. The true cost of this data collection is associated with retention expectations combined with privacy concerns (Mateescu, Rosenblat, & Boyd, 2016). This technology can allow border agents to become more effective in the screening process and increase the quantity of individuals to be cleared or turned away. The use of this technology in airports can identify suspects on the terror watch list and no fly watch list. A merger or blending of fixed surveillance and portable surveillance can reasonably reduce the time frame it takes to coordinate a safe and reasonable response from the agency involved.

RECOMMENDATION

There has been significant improvement in the field of facial recognition technology. The use of finger prints, retina scans, and DNA has been used to verify the identity of the generic population for over a decade at this point. The emerging field of facial recognition is not considered an exact science, but a merging of science and art.

The proper application and implementation of facial recognition technology will strengthen reasonable suspicion contacts. The alternative applications involving partnerships with stakeholders can provide quicker recoveries involving amber alerts, silver alerts, run away and kidnapping victims. The active mobile facial recognition technology can significantly increase the safety involving officer awareness when making initial contacts due to alerts generated by the facial recognition technology. Concerns involving invasion of privacy are limited due to public nature of law enforcement. The concern involving the disproportionate statistical matches involving minorities does not consider the evolution of the technological advances over time. This concern is additionally alleviated when considering the decision to arrest is not solely based upon the activation of a facial recognition alert. The cost of this technology will decrease with time while the accuracy increases with time. The application will also reduce the incorrect release of prisoners. Facial recognition technology should be actively implemented with law enforcement applications.

REFERENCES

Falk, K. (2007, July). Putting a name to a face: Facial recognition systems help officers make timely decisions. *Law Enforcement Technology*, *7,* 34-40. Retrieved from https://www.officer.com/magazine

Gaidos, S. (2013, August 27). Familiar faces: 'Super recognizers' never forget a visage, an unusual ability that can be put to good use. *Science News, 184*(5). doi: 10.1002/scin.5591840515

Gier, V., Kreiner, D., & Lampinen, J. (2016). Factors affecting recognition of senior citizens in a silver alert. *Journal of Police and Criminal Psychology 32*(3), 185-196. Retrieved from https://link.springer.com/journal/11896

Gross, G. (2017, March 23). US lawmakers question police use of facial recognition tech. *NetworkWorld*. Retrieved from https://www.networkworld.com/article/3183431/us-lawmakers-question-police-use-of-facial-recognition-tech.html

Kepple, K., Epstein, M., & Grisham, L. (2014, September 23). By the numbers: Missing persons in the USA. *USA Today*. Retrieved from https://www.usatoday.com/story/news/nation-now/2014/09/23/missing-persons-children-numbers/16110709/

Massola, J., & Preiss, B. (2017, October 16). New facial recognition database: Surveillance/privacy concerns. *The Age*. Retrieved from https://www.theage.com.au/

Mateescu, A., Rosenblat, A., & Boyd, D. (2016). Dreams of accountability, guaranteed surveillance: The promises and cost of body worn cameras. *Surveillance and Society, 14*(1), 122-127. doi: 10.24908/ss.v14i1.6282

Rodriquez, R. (2016, September). Facial recognition: Art or science? *Law & Order; Wilmette* Vol.64, Issue 9 (36-39).

Sofge, E. (2013, December 17). The end of anonymity. Technology that matches faces to names can already single out criminals. What happens when it can identify anyone? *Popular Science*, 46-53.

Taylor, M. (2017, March 13). The Art of Facial Recognition. *Forensic Magazine; Rockaway* (5).

Weiss, J., & Davis, M. (2005, October). Facial recognition technology in law enforcement. *Law & Order, 53*(10), 100-106. Retrieved from http://www.hendonpub.com/resources/article_archive/results/details?id=5900

Wolford, E. (2009, June). Not just another face in the crowd. *Security Magazine.* Retrieved from https://www.securitymagazine.com/articles/79821-not-just-another-face-in-the-crowd-1