Facial Recognition – Frequently Asked Questions

Prepared September 2019

Question: What is the Statewide Network of Agency Photos (SNAP)?

Answer: The SNAP is the central repository for storing the State of Michigan's digital facial images. These images include arrestee, Michigan Department of Corrections, and Michigan Department of State images and identifying data (e.g., name, date of birth, etc.) for law enforcement access.

Question: What is the role of the SNAP Unit?

Answer: The SNAP Unit employs trained facial examiners who can assist investigators from state, local, and federal law enforcement agencies with digital photo lineups and FR searches.

Question: What training do MSP facial examiners receive on the use of FR technology?

Answer: MSP facial examiners receive a minimum of 40 hours of training on facial comparison and identification. Facial examiners receive certificates of training from the Federal Bureau of Investigation and Ideal Innovations, Inc. This training adheres to the standards set forth by the Organization of Scientific Area Committees for Forensic Science and Facial Identification Scientific Working Group.

Question: What is facial recognition (FR)?

Answer: FR is an automated process for comparing faces.

Question: How does FR Work?

Answer: Computer software uses an algorithm to generate a unique template (map) of a face. The software then compares that template against templates of other faces contained in a database, typically resulting in a group of facial images ranked according to computer evaluated similarity.

Question: Is FR a form of positive identification?

Answer: No. Per MSP policy, FR is not considered to be a form of positive identification. It is considered to be an **investigative lead only**, requiring the investigator to continue the criminal investigation before making any final determinations, up to and including arrest.

Question: How accurate is FR?

Answer: There are two factors that determine the accuracy of FR: algorithm and human performance. The MSP relies on the results of the current National Institute of Standards and Technology (NIST) Face Recognition Vendor Test which tests FR algorithm performance. Human performance is determined by evaluating facial examiner training, experience, and the results of competency and proficiency testing.

In 2018, the NIST conducted the most comprehensive examination to date comparing the accuracy of state-of-the-art face recognition algorithms to human experts. The findings

demonstrated neither gets the best results alone. Maximum accuracy was achieved with a collaboration between the two.

Question: Does the quality of the photo(s) searched impact the results of a FR search?

Answer: Yes. Important factors that can impact the outcome of a FR search include: image collection (i.e., compression, camera position), image capture (i.e., moiré, perspective, aspect ratio, lighting), subject pose, facial expression, and obstructions to include eyewear, hair, clothing, etc.

Question: What are common misconceptions related to law enforcements' use of FR technology?

Answer:
False Positives
Because FR is not considered to be positive identification, the FR tools will never provide a "false positive" match, as "positive matches" are never returned to investigators; only investigative lead reports. All investigative leads are peer reviewed by trained facial examiners prior to being released to investigators.

All biometrics are statistical in nature and return search results, which are based on a likelihood score. Likelihood scores never guarantee a match but imply the strength of the likelihood. Face scores always require an examiner to review the results regardless of the score.

Real-time Screening
The MSP does not own the technology to perform FR resulting from a live video feed. This means the MSP is not capable of doing something like scanning a crowd at a public place and identifying people who are in attendance in real-time. Everything the SNAP Unit does is after-the-fact and must have a criminal nexus, which is verified through a criminal complaint number or valid purpose code. The MSP is using FR as a post-incident forensic tool to enable detectives to generate investigative leads in criminal investigations.

Racial, Skin, Gender Bias
The proprietary FR algorithms used by the MSP return results based on facial measurements, not skin color or gender. Most FR algorithms produce a range of soft biometrics. For example: sex, race, age, expression, etc. The MSP does not use soft biometrics for searching or as part of the examination process because this could introduce bias into the process.

Question: How is the MSP using FR?

Answer: The MSP has been using automated FR since 2001 to support criminal investigations. FR is used to identify subjects without identification on a traffic stop and can assist detectives in developing a suspect in a criminal investigation when surveillance video or other suspect images are available. Additionally, FR technology is being used to detect potential fraud within the MSP copy of the MDOS database.

Question: Why is the MSP performing FR searches of driver license and personal identification card images?

Answer: The MSP seeks to enhance public safety by utilizing FR technology to facilitate the identification of unknown subjects and to deter and prevent identity fraud.

Question: What happens if my driver's license or personal identification card image is one of the results returned by the FR search?

Answer: A trained facial examiner manually compares the unknown image against the images returned by the software. The examiner, not the computer, decides if any of the result images are similar enough to the unknown image to move forward with an investigation.

Question: Is the MSP using real-time video FR to track or conduct surveillance on individuals?

Answer: No. The MSP does not have the ability to access real-time video while performing FR simultaneously. All FR searches being conducted occur after the crime has been committed.

Question: How are other agencies using and not using the MSP FR tool?

Answer: Approved law enforcement agencies in the state of Michigan can use the MSP FR tool in the following ways:

1. They can submit a request for a FR search to the MSP SNAP Unit in which a trained facial examiner will conduct the search on their behalf.

2. They can request access to the MSP SNAP FR desktop tool to conduct their own searches. In these cases, searches are conducted against the mugshot/arrestee database only (not the MDOS images). The MSP recommends all FR searches be conducted by personnel who are trained on facial comparison and identification.

3. They can search a live capture photo using the MSP Mobile FR solution.
NOTE: Mobile FR is not used for or capable of real-time screening.

Law enforcement agencies can also purchase their own FR solution. In these cases, any searches conducted are only capable of searching the agency's own internal mugshot databases.

Question: Does the MSP have policies and procedures in place to ensure people are not abusing the FR tool?

Answer: Yes. The MSP and approved users of the MSP FR tool adhere to an Acceptable Use Policy that addresses auditing and penalties for misuse. Additionally, the MSP conducts random and targeted audits to ensure compliance with the policy. To date, there have been no reports of misuse pertaining to the MSP's use of FR.

The SNAP Acceptable Use Policy establishes procedures for acceptable use of the images, information, and tools within the SNAP system. This policy addresses disclosure and use of information, auditing, and penalties for misuse. The MSP's policy was cited six times in the 2016 Georgetown Law Center on Privacy and Technology Report (commonly referred to as the Georgetown Report) as the basis for their policy recommendations.

In 2018, the Michigan Office of the Auditor General (OAG) sent a team of auditors to the MSP for several weeks to assess the SNAP program to include the FR program. The auditors conducted a thorough review of all processes to ensure staff is complying with policies, procedures, and best practices. The team's preliminary review did not identify any concerns that would warrant the need for conducting a full audit; thus, the planned performance audit was terminated at the direction of the OAG.

Question: What is the legal authority for the MSP to store and use mugshot photos for the purpose of using FR?

Answer: MCL 28.248 Use of biometric data for criminal identification.
Section 8. Biometric data obtained under a law or rule for noncriminal identification purposes may be used for criminal identification purposes unless prohibited by law or rule.

MCL 28.243 Collecting and forwarding biometric data of person arrested; manner; destruction of biometric data and arrest card; compliance with subsection (8); duties of clerk on final disposition of charge; contents of report; informing director of Federal Bureau of Investigation; requirements applicable to arrest where charges dismissed before trial; comparison of biometric data with that on file; informing arresting agency and prosecuting attorney; applicability of provisions; prohibited conduct under subsection (5).

Question: What is the legal authority for the MSP to store and use driver license or personal identification photos for the purpose of using FR?

Answer: MCL 257.307 (2) (a)
(2) An applicant for an operator's or chauffeur's license may have his or her image and signature captured or reproduced when the application for the license is made. The secretary of state shall acquire equipment purchased or leased under this section under standard purchasing procedures of the department of technology, management, and budget based on standards and specifications established by the secretary of state. The secretary of state shall not purchase or lease equipment until an appropriation for the equipment has been made by the legislature. A digital photographic image and signature captured under this section must appear on the applicant's operator's license or chauffeur's license. A person's digital photographic image and signature shall be used as follows:

(a) By a federal, state, or local governmental agency for a law enforcement purpose authorized by law.

Question: How does the MSP address privacy concerns?

Answer: All information contained within the SNAP system is transmitted, used, disseminated, and disposed of in accordance with state and federal laws, rules, policies, and regulations. These include, but are not limited to, the most recent federal Criminal Justice Information Systems (CJIS) Security Policy, the Michigan CJIS Security Addendum, the CJIS Policy Council Act (1974 PA 163), MCL 28-211-28.216, and the most current CJIS Administrative Rules.

Question: How would a ban on FR impact law enforcement?

Answer: If law enforcement lost the ability to use FR, facial examiners would be forced to analyze images manually, resulting in lengthy, inefficient, and costly investigations. The resulting investigative delays would put the public at a greater risk of victimization.

Question: Where can I find more information on FR?

Answer: The following links are provided for awareness purposes:

MSP SNAP Unit and Acceptable Use Policy - https://www.michigan.gov/msp/0,4643,7-123-72297_64747_64749-357133--,00.html

Facial Identification Scientific Working Group (FISWG) - https://fiswg.org/documents.html

Rank One Computing's Automated Face Recognition Blog - https://blog.rankone.io/

The Georgetown Law Center on Privacy and Technology's Georgetown Report - https://www.law.georgetown.edu/privacy-technology-center/publications/the-perpetual-line-up/

NIST Face Recognition Vendor Test (FRVT) Ongoing - https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

NIST Black Box Study - https://www.nist.gov/news-events/news/2018/05/nist-study-shows-face-recognition-experts-perform-better-ai-partner