

# Facial Recognition

## 471.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the use of Facial Recognition (FR) software by the Fontana Police Department.

The Fontana Police Department considers the results, if any, of a facial recognition search to be advisory in nature as an investigative lead only. Facial recognition search results are not considered positive identification of a subject and do not, on their own, establish probable cause without further investigation. Any possible connection or involvement of the subject(s) to the investigation must be determined through further investigative methods.

### 471.1.1 DEFINITIONS

**Facial Recognition (FR)** software compares patterns within the field of computer vision. Such approaches do not rely upon intrinsic models of what a face is, how it should appear, or what it may represent. In other words, the matching is not based on biological or anatomical models of what a face—or the features that make up a face—look like. The patterns used in FR algorithms do not correlate to obvious anatomical features such as the eyes, nose or mouth in a one-to-one manner, although they are affected by these features.

**Candidate Images**—The possible results of a facial recognition search. When facial recognition software compares a probe image against the images contained in a repository, the result is a list of most likely candidate images that were determined by the software to be sufficiently similar to or most likely resemble the probe image to warrant further analysis. A candidate image is an investigative lead only and does not establish probable cause to obtain an arrest warrant without further investigation.

**Facial Recognition Software/Technology**—Third-party software that uses specific proprietary algorithms to compare facial features from one specific picture—a probe image—to many others (one-to-many) that are stored in an image repository to determine most likely candidates for further investigation.

**Investigative Lead**—Any information which could potentially aid in the successful resolution of an investigation, but does not imply positive identification of a subject or that the subject is guilty of a criminal act.

**One-to-Many Face Image Comparison**—The process whereby a probe image from one subject is compared with the features of reference images contained in an image repository, generally resulting in a list of most likely candidate images.

**Unsolved Image File**—A lawfully obtained probe image of an unknown suspect may be added by authorized law enforcement users to an unsolved image file pursuant to an authorized criminal investigation and if a search has produced no candidates and the subject remains unknown. Images in an unsolved image file are periodically compared with the known images in an image repository.

## *Facial Recognition*

---

**Valid Law Enforcement Purpose**— FR is to be used for information/intelligence gathering, development, or collection, use, retention, or sharing that furthers the authorized functions and activities of a law enforcement agency, which may include the prevention of crime, ensuring the safety of the public, protection of public or private structures and property, furthering officer safety, while adhering to law and agency policy designed to protect the public.

### **471.2 POLICY**

Facial recognition technology involves the ability to examine and compare distinguishing characteristics of a human face through the use of biometric algorithms contained within a software application. This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce an imminent threat to health or safety, and help in the identification of persons unable to identify themselves or deceased persons. The Fontana Police Department has established access and use of a facial recognition software system to support investigative efforts. The software will be treated as any other investigative lead and should never be used as a sole guarantee or for probable cause to arrest.

This policy will provide the Fontana Police Department personnel with guidelines and principles for the collection, access, use, dissemination, retention, and purging of images and related information applicable to the implementation of a facial recognition (FR) program. This policy will ensure that all FR uses are consistent with authorized purposes while not violating the privacy, civil rights, and civil liberties of individuals. This facial recognition policy assists the Fontana Police Department and its personnel in:

- (a) Increasing public safety and improving security.
- (b) Minimizing the threat and risk of injury to the public.
- (c) Minimizing the threat and risk of physical injury or financial liability to law enforcement and others responsible for public protection, safety, or health.
- (d) Minimizing the potential risks to individual privacy, civil rights, civil liberties, and other legally protected interests.
- (e) Protecting the integrity of criminal investigatory and justice system processes.
- (f) Minimizing the threat and risk of damage to real or personal property.
- (g) Fostering trust by strengthening transparency, oversight, and accountability.
- (h) Making the most effective use of public resources.

### **471.3 USE OF FACIAL RECOGNITION**

All deployments of the facial recognition system are for official use only and are law enforcement sensitive. The provisions of this policy are provided to support the following authorized uses of facial recognition information.

## *Facial Recognition*

---

- (a) A reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in or planning criminal conduct or activity that presents a threat to any individual or the community.
- (b) An active or ongoing criminal investigation.
- (c) To mitigate an imminent threat to health or safety of the community.
- (d) To assist in the identification of a person who lacks the capacity or is otherwise unable to identify themselves (such as an incapacitated, deceased, or otherwise at-risk person).
- (e) To investigate and/or corroborate tips and leads.
- (f) For a person who an officer reasonably believes is concealing his or her true identity and has a reasonable suspicion the individual has committed a misdemeanor or felony crime other than concealing his or her identity.
- (g) For persons who lack the capacity or are otherwise unable to identify themselves and who are a danger to themselves or others.

### **471.3.1 FACIAL RECOGNITION ACCESS**

Authorized access to a facial recognition system will be granted only to personnel whose positions and job duties require such access and who have successfully completed the required training. Personnel will be provided individual usernames and passwords to the facial recognition system that are not transferrable, must not be shared, and must be kept confidential.

### **471.4 PROHIBITED USES**

The Fontana Police Department will prohibit access to and use of the facial recognition system, including dissemination of facial recognition search results, for the following purposes:

- (a) Non-law enforcement (including but not limited to personal purposes).
- (b) Any purpose that violates the U.S. Constitution or laws of the United States, including the protections of the First, Fourth, and Fourteenth Amendments.
- (c) Prohibiting or deterring lawful individual exercise of other rights, such as freedom of association, implied by and secured by the U.S. Constitution or any other constitutionally protected right or attribute.
- (d) Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

The Fontana Police Department will not connect the facial recognition system to any interface that performs live video surveillance, including surveillance cameras, drone footage, and body-worn cameras (California Assembly Bill 1215).

## *Facial Recognition*

---

### **471.5 FACIAL RECOGNITION ADMINISTRATOR**

Primary responsibility for the operation of the Fontana Police Department's facial recognition program and system, operations, and the coordination of personnel; the receiving, seeking, retention, evaluation, data quality, use, purging, sharing, disclosure, or dissemination of information; and the management is assigned to the Special Operations Division Commander or their designee.

The Special Operations Division Commander will be responsible for the following responsibilities:

- (a) Managing the facial recognition program to ensure compliance with applicable laws, regulations, standards, and policy.
- (b) Acting as the authorizing official for individual access to facial recognition information.
- (c) Ensuring that user accounts and authorities granted to personnel are maintained in a current and secure "need-to-know" status.
- (d) Ensuring that random audits of user compliance with system requirements and the entity's facial recognition policy and applicable law are conducted and documented.
- (e) Ensuring and documenting that personnel meet all prerequisites stated in this policy prior to being authorized to use the facial recognition system.

### **471.6 FACIAL RECOGNITION SERVICES**

The Fontana Police Department will contract with facial recognition software service companies to provide software and system development services for the department's facial recognition system.

The Fontana Police Department will perform facial recognition searches utilizing mug-shot images, also known as booking photos. The booking photos are lawfully obtained from known offenders when they are arrested and booked by law enforcement.

The Fontana Police Department will contract only with commercial facial recognition companies that provide assurances that their methods for collecting, receiving, accessing, disseminating, retaining, and purging face recognition information comply with applicable local, state, tribal, territorial, and federal laws, statutes, regulations, and policies and that these methods are not based on unfair or deceptive information collection practices.

### **471.7 INVESTIGATIVE LEADS**

The Fontana Police Department considers the results, if any, of a facial recognition search to be advisory in nature as an investigative lead only. Facial recognition search results are not considered positive identification of a subject and do not, on their own, establish probable cause without further investigation. Any possible connection or involvement of the subject(s) to the investigation must be determined through further investigative methods.

Investigative leads will need to be vetted with supervisory oversight. Personnel will need to establish their own probable cause before making an arrest. In any case where facial recognition software was used as an investigative lead, the employee's supervisor will review the case in

### *Facial Recognition*

---

order to ensure the AFR was used as an investigative lead and not solely to establish probable cause for an arrest.

#### **471.8 TRAINING**

Before access to the facial recognition system is authorized, personnel must receive familiarization training and acknowledge the applicable policies and procedures. Members will receive department-approved training for those authorized to use or access the facial recognition software system.

#### **471.9 USER AUDITS**

The Fontana Police Department's Special Operations Division Commander will maintain an audit report of requested, accessed, searched, or disseminated automated facial recognition information.