EASTHAMPTON POLICE DEPARTMENT	Department Manual: Policy No. 4.31
SUBJECT: FACIAL RECOGNITION	
MASSACHUSETTS POLICE ACCREDITATION STANDARDS REFERENCED: 42.2.13	GENERAL ORDER
Issue Date: 01-24-2023 Effective Date: 01-24-2023 Revision Date:	Issuing Authority Robert J. Alberti Robert J. Alberti CHIEF OF POLICE

PURPOSE

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.

It is the purpose of this policy to provide Easthampton Police Department personnel with guidelines and principles regarding the utilization of facial recognition technology. This policy will ensure that all facial recognition uses are consistent with authorized purposes while not violating the privacy, civil rights, and civil liberties of individuals.

All facial recognition searches are law enforcement sensitive/for official use only/ (LES/FOUO).

POLICY

A. It is the policy of the Easthampton Police Department to request facial recognition searches using facial recognition technology only through a written request submitted to the Registrar of Motor Vehicles, the Department of State Police, or the Federal Bureau of Investigation.

B. It is the policy of the Easthampton Police Department to only perform a facial recognition search that is consistent with this policy and the law.

C. It is the policy of this Department to document each facial recognition search and to ensure that such documentation is submitted quarterly to the Executive Office of Public Safety and Security (EOPSS) as required by law.

D. It is the policy of this Department to comply with all federal, state, and local laws and regulations regarding the use of facial recognition technology.

DEFINITIONS

A. **Authorized Agency:** Includes the Registrar of Motor Vehicles, the Department of State Police, and the Federal Bureau of Investigation.

B. **Biometric Data:** Computerized data relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of such person, including, but not limited to, facial recognition, fingerprints, palm veins, deoxyribonucleic acid, palm prints, hand geometry or iris recognition.

C. **Biometric surveillance system:** Any computer software that performs facial recognition or other remote biometric recognition.

D. **Facial recognition:** An automated or semi-automated process that assists in identifying or verifying an individual or capturing information about an individual based on the physical characteristics of an individual's face, head or body, that uses characteristics of an individual's face; provided, however that "facial recognition" shall not include the use of search terms to sort images in a database.

E. **Facial recognition search:** A computer search using facial recognition to attempt to identify an unidentified person by comparing an image containing the face of the unidentified person to a set of images of identified persons; provided, however, that a set of images shall not include moving images or video data.

F. **Lead:** For the purposes of this policy only, situations where investigative follow up has determined that there are reasonable grounds to believe that two photos are in fact one in the same person.

G. **Other remote biometric recognition:** An automated or semi-automated process that assists in identifying or verifying an individual or capturing information about an individual based on an individual's gait, voice or other biometric characteristic or that uses such characteristics to infer emotion, associations, activities or the location of an individual; provided, however, that "other remote biometric recognition" shall not include the identification or verification of an individual using deoxyribonucleic acid, fingerprints, palm prints or other information derived from physical contact.

PROCEDURES

I. APPLICABILITY

A. This policy applies to the Easthampton Police Department's utilization of facial recognition technology.

B. This policy does not apply to the Department's acquisition, possession, and use of personal electronic devices, such as cell phones or tablets that utilize facial recognition technology for the sole purpose of user authentication.

C. This policy does not apply to the Department's acquisition, possession, and use of automated video or image redaction software; provided, that such software does not have the capability of performing facial recognition or other remote biometric recognition.

D. This policy does not limit the Department's ability to receive evidence related to the investigation of a crime derived from a biometric surveillance system; provided, that the use of a biometric surveillance system was not knowingly solicited by or obtained with the assistance of

a public agency or any public official in violation of any section or subsection of this policy or relevant law.

II. PERMITTED USE

Authorized Easthampton Police Department personnel may only perform or request a facial recognition search in the following instances:

A. To execute an order, issued by a court or justice authorized to issue warrants in criminal cases, based upon specific and articulable facts and reasonable inferences therefrom that provide reasonable grounds to believe that the information sought would be relevant and material to an ongoing criminal investigation or to mitigate a substantial risk of harm to any individual or group of people; and

B. Without an order to identify a deceased person or if the law enforcement agency reasonably believes that an emergency involving substantial risk of harm to any individual or group of people requires the performance of a facial recognition search without delay. Any emergency request shall be narrowly tailored to address the emergency and shall document the factual basis for believing that an emergency requires the performance of a facial recognition search without delay.

III. PROCESS FOR THE UTILIZATION OF FACIAL RECOGNITION TECHNOLOGY

A. **Process for Requesting Facial Recognition Searches**

1. Requests for facial recognition searches shall be submitted to the authorized agencies, with photograph(s) to be reviewed, the incident number, the crime type, and such other pertinent information as may or may not be required by the authorized agencies. Photographs shall be handled as specified in the Department policy on Evidence Property.

2. Easthampton Police Department personnel shall comply with all applicable policies, procedures, and protocols as established by the authorized agencies in requesting facial recognition searches.

B. **Status of Facial Recognition Search Results:** Any results from a facial recognition search will be provided to the Department as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF

ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.

IV. PROHIBITED USES

A. **Surveillance:** Easthampton Police Department personnel shall not use facial recognition to surveil the public through any camera or video device.

B. **First Amendment Events:** The Department and its personnel shall not violate the First, Fourth, and Fourteenth Amendments and will not perform or request facial recognition searches about individuals or organizations based solely on the following:

1. Their religious, political, or social views or activities;

2. Their participation in a particular noncriminal organization or lawful event; or

3. Their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, gender identities, sexual orientations, or any other classification protected by law.

C. **Facial Recognition Use for Immigration Enforcement:** Department members are strictly prohibited from using facial recognition to assess immigration status.

V. GOVERNANCE & OVERSIGHT

A. **Authorized Department Personnel:** The Department's Detective Lieutenant will determine, consistent with this policy, which Department personnel will be authorized to submit requests for facial recognition searches.

B. **Facial Recognition Administrator:** The Department's Detective Lieutenant will be the facial recognition administrator and will be responsible for the following:

1. Ensuring that the Department and its personnel remain in compliance with applicable laws, regulations, standards, and policy regarding facial recognition.

2. Acting as the authorizing official for Department personnel requests for facial recognition searches.

3. Ensuring that Department personnel receive the necessary training specified in this policy prior to being authorized to submit requests for facial recognition searches.

4. Confirming, through random audits, that facial recognition information is purged in accordance with this policy and to ensure compliance with applicable laws, regulations, standards, and policy.

C. **Privacy, Civil Rights, and Civil Liberties:** The Easthampton Police Department is guided by applicable laws, regulations, and standards to ensure that privacy, civil rights, and civil liberties are not violated by this facial recognition policy or by Department personnel.

D. **Mandatory Reporting**

1. The Department shall document each facial recognition search performed and shall ensure that such documentation is submitted quarterly to the Executive Office of Public Safety & Security (EOPSS). Such documentation shall include:

   a. a copy of any written request made for a facial recognition search;
   b. the date and time of the request;
   c. the number of leads generated, if any;
   d. the database searched;
   e. the name and position of the requesting officer;
   f. the reason for the request, including, but not limited to, any underlying suspected crime;
   g. the entity to which the request was submitted; and
   h. data detailing the individual characteristics included in the facial recognition request.

2. Such documentation shall not be a public record, except for as provided for in G.L. c. 6, section 220(d).

VI. INFORMATION RETENTION

A. Once a facial recognition image is downloaded by Department personnel and incorporated into a criminal intelligence record or an investigative case file, the facial recognition information is then considered criminal intelligence or investigative information, and the laws, regulations, and

policies applicable to that type of information or criminal intelligence govern its use.

B. Any images that do not originate with the Department will remain in the custody and control of the originating agency and will not otherwise be transferred to any other entity.

C. Probe images and face recognition search results are saved within the Department's system audit log for audit purposes only, consistent with the law and this policy. The audit log is available only to the Detective Lieutenant and will be purged annually. The audit log is not searchable and face recognition searches cannot be performed using the audit log.

VII. TRAINING

Prior to being authorized to perform or request a facial recognition search, Department personnel must complete training that addresses the following topics:

A. Department responsibilities and obligations under applicable federal, state, or local law and policy.

B. Privacy, civil rights, and civil liberties protections on the use of the technology and the information received.

C. Conditions and criteria under which the face recognition searches may be requested.

D. Face recognition system functions, limitations, and interpretation of results.

E. Use of face recognition search results as investigative leads only.

F. Mechanisms for reporting violations of the Department facial recognition policy.

G. The nature and possible penalties for facial recognition policy violations, including dismissal, criminal liability, and immunity, if any.

H. Any applicable operational policies.