Facial Recognition

Model Policy

December 2019

New York State | Municipal Police Training Council

New York State Division of Criminal Justice Services
80 South Swan Street, Albany, New York 12210

www.criminaljustice.ny.gov

Facial Recognition

Model Policy

Copyright Notice

Facial Recognition Model Policy

The Facial Recognition Model Policy is intended to allow for the individual needs of each of the police departments in New York State regardless of size or resource limitations. Law Enforcement are encouraged to customize these protocols to meet their regional needs, while being mindful of the intent of the policy. As with all model policies adopted by the Municipal Police Training Council (MPTC), this policy is non-binding upon agencies within New York State and is meant to serve as a guide to be used in developing a department's individual policy.

The Municipal Police Training Council (MPTC) approved the model policy during their December 2019 meeting.

Acknowledgements

The New York State Division of Criminal Justice Services (DCJS) acknowledges the extensive work done by the following associations and agencies:

Law Enforcement Training Directors' Association of New York State

New York State Association of Chiefs of Police

New York State Police

New York City Police Department

New York State Sheriff's Association

State University of New York

District Attorneys Association of New York

High Intensity Drug Trafficking Areas (HIDTA)

Facial Recognition Model Policy
Municipal Police Training Council

I   Purpose

The purpose of this policy is to provide guidance to law enforcement agencies in developing written policies and procedures regarding the use of facial recognition technology. The policy promotes public safety and efficiency of law enforcement criminal investigatory activities through the use of facial recognition technologies and protocols, while ensuring the appropriate safeguards are in place to protect the privacy, civil rights and civil liberties of individuals. This policy is intended to allow for the individual needs of police agencies in New York State regardless of size or resource limitations. Law enforcement agencies are encouraged to customize these protocols to meet their agency's needs, while being mindful of the intent of the policy.

II   Policy

Facial recognition technology can be used to enhance public safety by assisting law enforcement with identification of unknown subjects. The technology should be used in a manner that protects the civil rights and civil liberties of citizens, including those rights guaranteed by the First, Fourth, and Fourteenth Amendments of the United States Constitution. Results obtained utilizing the facial recognition software are merely a lead and are not probable cause to arrest. A further investigation is needed to develop probable cause to arrest.

III   Definitions

A. **"Facial recognition"-** the automated searching of a facial image against a database of biometric templates, which may result in a group of potentially matching facial images ranked by computer-evaluated similarity (i.e., one-to-many matching).

B. **"Examiner"-** An individual who has, at minimum, received training on how to use the facial recognition software, possesses knowledge and understanding of the agency's facial recognition policy and procedures, and an understanding of applicable laws and privacy protections.

C. **"Facial recognition software"-** a software program or other tool that incorporates one or more automated processes to perform facial recognition.

IV   Permissible Use of Facial Recognition Technologies

A.   Examiners are the only individuals authorized to conduct facial recognition utilizing facial recognition software.

B.   Examiners are only authorized to utilize facial recognition software to:

     1.   Attempt to identify an individual(s) when such individual(s):

         a.   has committed a criminal offense; or

         b.   is involved in or is planning definable criminal conduct or activity; or

         c.   is a possible missing person, crime victim, or witness to criminal activity; or

         d.   is deceased; or

         e.   is incapacitated and unable to communicate; or

         f.   is under arrest and:

             (i)   does not possess valid identification;

             (ii)   is not forthcoming with valid identification; or

             (iii)   appears to be using someone else's identification or false identification.

     2.   Prevent, detect, and/or assess potential safety threats to members of the public and/or public officials.

C.   Images contained in the facial recognition software database used to search against images submitted for identification must be lawfully obtained such as criminal history photographs that are not sealed or otherwise protected from such use.[1]

D.   Members of a law enforcement agency may submit to the examiner images that originate from a lawful source, including law enforcement personnel and private citizens, for performance of facial recognition

---

[1] New York/New Jersey HIDTA utilizes verified criminal mugshot source images. The facial recognition software and database is available to all New York local and state law enforcement agencies via the eJustice Portal.

provided that the images are relevant to an authorized purpose delineated in section IV B.

E.   All computer-generated potential matches between a subject displayed in a submitted image and an identifiable person shall be visually evaluated by an examiner.

   1.   Examiners will determine whether similarity exists between the subject and the identifiable person, through a manual or visual review of facial features such as the eyes, ears, nose, mouth, chin, lips, eyebrows, hair/hairline, scars, marks, and tattoos, to justify reporting an investigative lead.

   2.   When practicable, a second examiner should review any potential identifications determined by the first examiner.

   3.   Potential identifications made using facial recognition software shall be considered investigative leads only and shall not be deemed positive identification.

   4.   Law enforcement personnel who receive facial recognition search results should be advised that such results are investigative leads only and do not establish probable cause to arrest, and should not be used as the sole basis for any warrant application.

F.   Examiners may accept the submission of images from another law enforcement agency, in an attempt to identify individuals through the use of facial recognition technology, provided the following requirements are met:

   1.   All permissible and prohibited uses of this policy are adhered to; and

   2.   Acknowledgement to the submitting agency that a facial recognition result is only an investigative lead and is not subject to be considered a positive identification of any subject.

G.   Facial recognition search results, including personal information regarding potential identifications, may be disseminated to any law enforcement agency or official with a need to know such information in the performance of official duties, provided the dissemination is for an authorized use as delineated in Section IV B and is subject to all Federal and New York State Laws on privacy, confidentiality and dissemination.

V   Prohibited Use

A.   The use of Facial Recognition software is restricted to approved legitimate law enforcement purposes as outlined in this policy. Use of Facial Recognition software for personal or other non-official purposes is a violation of this policy.

B.   Facial recognition software shall not be used to identify any individual when the request for identification is based on images that were obtained by unlawful means and based <u>solely</u> upon the individual's:

1.   Religious, political, or social views or activities;

2.   Participation in a noncriminal organization or lawful event; or

3.   Race, creed, color, national origin, sex, marital status, sexual orientation, gender identity expression, disability, or any other protected characteristic recognized under Article 4 of the New York Civil Rights Law.

VI   Records

A.   All records, data, and information received or generated through any permissible use of facial recognition technology, including facial recognition requests and images received, screenshots, printouts, and facial recognition software output, shall be maintained for audit purposes and conform to the provisions of an agency's privacy policy and record retention policies.

B.   Outputs of the facial recognition software will be provided to the requestor for inclusion with the case file.

C.   Procedures and practices to evaluate and monitor the use of facial recognition software and measure compliance of examiners with this policy, including the performance of periodic and random audits and/or inspections shall be instituted.

D.   Images submitted for identification should not become part of the searchable database but will be maintained as part of the investigative case file.

E.   Any and all disclosure of facial recognition data must be consistent with the agency's record release policy and applicable statutes regarding, but not limited to, evidence discovery and disclosure pursuant to the Freedom

of Information Law (FOIL). Any requests for such data should be reviewed by the agency's legal advisor.

VII   Training

A.   Examiners will, at a minimum, have received training on how to use the facial recognition software and knowledge and understanding of the agency's facial recognition policy and procedures including applicable laws and privacy protections.

B.   This policy is not intended to be a substitute for proper training in the use of facial recognition software.