Facial Recognition Model Policy
KRS 61.9305
Adopted 12/19/23

I. POLICY

A. Facial recognition technology must only be used for legitimate law enforcement purposes. The authorized uses for employing facial recognition technology are to produce investigative leads which may assist in the:

1. Identification of an individual when there is a good faith basis to believe that such individual has committed, or is committing a crime;

2. Identification of an individual when there is a basis to believe that such individual is a missing person, crime victim, or witness to criminal activity;

3. Identification of a deceased person;

4. Identification of a person who is incapacitated or otherwise unable to identify themselves;

5. Identification of an individual who is under arrest and does not possess valid identification, is not forthcoming with valid identification, or who appears to be using someone else's identification or a false identification; or

6. Mitigation of an imminent threat to health or public safety.

B. The result of a facial recognition search is not considered a positive identification and, in the event of a criminal investigation, does not establish probable cause to arrest or obtain a search warrant, but merely serves as an investigative lead. The officer or investigator assigned to the case must establish, through other corroborating evidence, that the result provided through a facial recognition search is the perpetrator in the alleged crime.

C. Facial recognition technology shall not be used to identify a person participating in constitutionally protected activities in public spaces unless there is probable cause to believe that an offense has been committed.

II. DEFINITIONS

A. "Facial recognition technology" means the use of algorithmic comparison of images of an individual's facial features for the purposes of verification or identification, unless used for the sole purpose of authentication in order to access a secure device or secure premises.

B. "Law enforcement agency" means any:

1. Public agency that employs a police officer as defined in KRS 15.420 or a special law enforcement officer as defined in KRS 61.900;

2. Public agency that is composed of or employs other public peace officers; and

3. Elected or appointed peace officer who is authorized to exercise powers of a peace officer as defined in KRS 446.010.

C. "Facial recognition examiner" means a member of the agency who has completed training in the operation of the facial recognition technology and who has been authorized by the agency head to conduct facial recognition analysis.

III. PROCEDURES

A. The agency head shall designate those investigators, officers, and analysts within the agency who have completed training in the use of facial recognition technology as facial recognition examiners.

B. Images submitted for comparison must be publicly available or lawfully acquired and must only be compared to publicly available or lawfully acquired images.

C. An officer, investigator, or analyst who determines that facial recognition analysis fits the authorized uses of such technology, as enumerated in this policy, must submit a request in writing that an analysis be conducted, and the request must be approved by the agency head or their designee.

D. Once approval is obtained, the image for comparison, also known as the probe photo, will be submitted to the agency's authorized facial recognition examiner.

E. The privacy of all persons shall be protected by excluding, redacting, blurring, or otherwise obscuring any content which would impact the privacy of persons in the image, including nudity or sexual conduct.

F. When a result is received through the process of facial recognition analysis, the facial recognition examiner shall do the following:

1. Conduct a visual comparison of the images with specific attention to facial features for the purpose of evaluating whether they represent the same person. During this process, the examiner shall compare facial characteristics (e.g., eyes, ears, nose, chin, mouth, hair, overall facial structure, any scars, marks, blemishes, or tattoos, etc.) and general characteristics, such as overall complexion, gender, and age.

2. After the initial evaluation, the images will be provided to a second trained facial recognition examiner who shall conduct an independent analysis.

3. A supervisor designated by the agency head shall conduct final review of the images and provide written concurrence or non-concurrence.

4. Documentation of each use of facial recognition technology shall be completed and maintained by the agency. These records shall include:

a. The probe photo;

b. A description of any changes made to the probe photo;
c. A summary of the results of the search, including if no results were returned;
d. The best candidate image returned from the search; and
e. Any other information used in the analysis.

IV. RELIABILITY AND NON-DISCRIMINATION

A. Only facial recognition algorithms that have been evaluated by the National Institute of Standards and Technology shall be utilized.

B. The technology used shall have a [INSERT % HERE] minimum accuracy standard for face matches in all demographic groups to ensure nondiscrimination against any demographic group with reference to a Face Recognition Technology Evaluation or a Face Analysis Technology Evaluation, whichever is appropriate, conducted by the National Institute of Standards and Technology.

V. DATA INTEGRITY AND RETENTION

A. Records of all facial recognition examinations will be retained in accordance with applicable law, including the rules regarding exculpatory evidence, the Kentucky Open Records Act, and record retention schedules.

B. Records of all facial recognition examinations shall be maintained and contemporaneously updated within the agency's records.

C. The agency shall routinely audit the use of the system to ensure compliance with the policy, including the prior uses of the technology.

D. Use and sharing of information related to any facial recognition technology with another law enforcement entity shall only occur once the agency seeking the information is able to verify in writing that such usage meets or exceeds the requirements of this policy.

VI. TRAINING

A. Before access to the facial recognition technology is authorized, the agency head will require that the individuals designated to be facial recognition examiners and others who access its data complete training that specifies procedures and processes to ensure all personnel who utilize facial recognition technology are knowledgeable about the technology adopted by the agency and are able to ensure compliance with the provisions of the policy adopted by the agency.

DISCLAIMER: Please note that the adoption of this model policy is not required by law and each agency should develop a policy that best suits its particular circumstances in consultation with its own legal representation. However, KRS 61.9305(4) does require that prior to the use of facial recognition technology, a law enforcement agency shall have a use policy in place and that policy and any revisions to that policy be forwarded to the Justice and Public Safety Cabinet within 30 days of its adoption or revision before an agency may utilize facial recognition technology.