AN ACT relating to use of facial recognition technology.

Be it enacted by the General Assembly of the Commonwealth of Kentucky:

➔SECTION 1. A NEW SECTION OF KRS CHAPTER 61 IS CREATED TO READ AS FOLLOWS:

(1) As used in this section:

(a) "Council" means the Kentucky Law Enforcement Council;

(b) "Facial recognition technology" means the use of algorithmic comparison of images of an individual's facial features for the purposes of verification or identification;

(c) "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; and

(d) "Model facial recognition technology policy" means the model policy developed and published by the council under this section, regarding the use of facial recognition technology.

(2) On or before January 1, 2023, the council shall create and make publicly available a model policy, which shall:

(a) Specify the authorized uses of facial recognition technology;

(b) Specify requirements for persons authorized to use facial recognition technology;

(c) Require a law enforcement agency to document instances in which facial recognition technology is used;

(d) Provide procedures for the confirmation of any initial findings generated by

facial recognition technology by a secondary examiner;

(e) Specify data integrity and retention policies applicable to the data collected by the organization, including:

1. Maintenance and updating of records used;

2. A routine audit schedule to ensure compliance with the policy;

3. How long the organization will keep the data; and

4. The processes by which data will be deleted;

(f) Specify data security measures applicable to facial recognition technology, including:

1. How data collected will be securely stored and accessed; and

2. Rules and procedures for sharing data with other entities, which ensure that those entities comply with the sharing agency's policy as part of the data-sharing agreement; and

(g) Specify training procedures and processes to ensure all personnel who utilize facial recognition technology or access its data are knowledgeable about and able to ensure compliance with the policy.

(3) A search result using facial recognition technology shall not alone constitute probable cause for arrest.

(4) Facial recognition technology utilized by a law enforcement agency pursuant to this section shall:

(a) Only be used to compare a publicly available or lawfully acquired image against a database of publicly available or lawfully acquired images;

(b) Meet a minimum accuracy standard for face matches in all demographic groups to ensure nondiscrimination against any demographic group. A facial recognition service shall be deemed to meet the requirements of this paragraph by having received an accuracy score of ninety-nine percent (99%) or better for true positives, within one (1) or more data sets relevant

to the application, across all demographic groups as evaluated by the Face Recognition Vendor Test conducted by the National Institute of Standards and Technology;

(c) Ensure there is a mechanism to produce a record of prior uses of facial recognition technology that can be used to audit and verify images and information used to make a match of a person;

(d) Protect the privacy of persons by excluding, redacting, blurring, or otherwise obscuring nudity or sexual conduct involving any identifiable person. The limitation established in this paragraph shall not apply to images made available to the facial recognition service provider by an authorized law enforcement agency seeking to protect a minor at risk of abuse, kidnapping, or other threats to a minor's life or safety; and

(e) 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.

(5) A law enforcement agency that uses facial recognition technology shall have a use policy in place prior to using the technology. No later than ninety (90) days after publication of the model facial recognition technology policy, all law enforcement agency policies shall meet or exceed the standards set forth in the model facial recognition technology policy. Agencies shall make their facial recognition technology use policies available to the public in written form or posted on their public Web site.

(6) Evidence collected through the use of facial recognition technology in violation of this section shall not be admissible in any criminal proceeding to prove the identity of a defendant identified by the use of facial recognition technology.