CHAPTER 147

(SB 176)

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) "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; and

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

(2) A working group on facial recognition technology is hereby created and shall be attached to the Justice and Public Safety Cabinet for administrative purposes. The working group shall be chaired by the secretary of the Justice and Public Safety Cabinet or his or her designee and composed of representatives from the following organizations as nominated by the secretary and appointed by the Governor:

(a) The Kentucky Association of Chiefs of Police;

(b) The Department of Criminal Justice Training;

(c) The Kentucky League of Cities;

(d) The Kentucky Association of Counties; and

(e) The Kentucky Sheriff's Association.

(3) On or before January 1, 2024, the working group established pursuant to subsection (2) of this section shall create and make publicly available a model policy for use by law enforcement agencies, which shall:

(a) Specify the authorized uses of facial recognition technology consistent with the law, including but not limited to:

1. How search results using facial recognition technology relate to establishing probable cause for arrests; and

2. The prohibition of using facial recognition technology 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;

(b) Specify requirements for persons within a law enforcement agency that are authorized to use facial recognition technology;

(c) Require a law enforcement agency to specify a process for the 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 processes that address:

1. Maintenance and updating of records used;

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

3. The length of time the organization will keep the data; and

4. The processes by which data will be deleted;

(f) Specify data security measures applicable to the law enforcement agency's use of 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;

(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;

(h) Specify a process that requires a law enforcement agency utilizing facial recognition technology to compare a publicly available or lawfully acquired image against a database of publicly available or lawfully acquired images;

(i) Specify a minimum accuracy standard for face matches in all demographic groups to ensure nondiscrimination against any demographic group with reference to a Face Recognition Vendor Test conducted by the National Institute of Standards and Technology;

(j) Provide a specific 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; and

(k) Provide a process that addresses the privacy of persons by excluding, redacting, blurring, or otherwise obscuring nudity or sexual conduct involving any identifiable person.

(4) A law enforcement agency that uses facial recognition technology shall have a use policy in place prior to using the technology. A law enforcement agency shall file a full copy of its policy or any revision of its policy with the Justice and Public Safety Cabinet within thirty (30) days of the adoption or revision.

(5) This section shall not apply to a generally available consumer product that includes facial recognition technology, provided that the facial recognition technology is intended only for personal or household use. A law enforcement agency shall not use facial recognition technology under this subsection for law enforcement purposes.

Signed by Governor April 8, 2022.