AN ACT relating to violations of privacy.

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

➔SECTION 1. A NEW SECTION OF KRS CHAPTER 454 IS CREATED TO READ AS FOLLOWS:

(1) As used in this section, unless context requires otherwise:

(a) 1. "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.

2. Biometric identifiers do not include:

a. Writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color;

b. Donated organs, tissues, or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency;

c. Information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996; or

d. Any X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose or treat an illness or other medical condition or to further validate scientific testing or screening;

(b) "Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not

include information derived from items or procedures excluded under the definition of biometric identifiers; and

(c) "Facial recognition technology" means computerized technology that helps in discerning and identifying human faces using biometrics to map facial features from a photo or video and comparing this information with a large database of recorded faces.

(2) It is unlawful, absent a court-approved warrant, for any state or local government agency, or an official thereof, to obtain, retain, request, access, or use:

(a) Facial recognition technology; or

(b) Information obtained from or by use of facial recognition technology.

(3) Once a person is accepted by law enforcement as being a missing person or child, facial recognition technology may be used if there is video or a real time feed available, provided a proven family member or court-approved guardian gives written consent for the use of facial recognition technology.

(4) Photographs taken by the Transportation Cabinet, or by any other agency, in order to issue operators' licenses or personal identification cards shall not be sold to any entity and shall not be provided to any state or local government agency for the purpose of using facial recognition technology without a warrant.

(5) A private entity in possession of biometric identifiers or biometric information shall develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three (3) years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information shall comply with its established retention schedule and destruction

guidelines.

(6) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

(a) Informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

(b) Informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

(c) Receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

(7) No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

(8) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:

(a) The subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;

(b) The disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;

(c) The disclosure or redisclosure is required by law; or

(d) The disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

(9) A private entity in possession of a biometric identifier or biometric information shall store, transmit, and protect from disclosure all biometric identifiers and biometric information:

(a) Using the reasonable standard of care within the private entity's industry; and

(b) In a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other sensitive information.

➔SECTION 2. A NEW SECTION OF KRS CHAPTER 411 IS CREATED TO READ AS FOLLOWS:

(1) Any violation of Section 1 of this Act constitutes an injury, and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandamus in any court of competent jurisdiction to enforce Section 1 of this Act.

(2) Any person who has been subjected to facial recognition technology in violation of Section 1 of this Act, or about whom information has been obtained, retained, accessed, or used in violation of Section 1 of this Act, may institute proceedings in any court of competent jurisdiction.

(3) A prevailing party may recover for each violation:

(a) Against an entity that negligently violates a provision of Section 1 of this Act, liquidated damages of one thousand dollars ($1,000) or actual damages, whichever is greater;

(b) Against an entity that intentionally or recklessly violates a provision of Section 1 of this Act, liquidated damages of five thousand dollars ($5,000) or actual damages, whichever is greater;

(c) Reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and

(d) Other relief, including an injunction, as the court may deem appropriate.

(4) The Attorney General may bring an action to enforce Section 1 of this Act. In any action brought by the Attorney General, a violation of Section 1 of this Act is subject to a civil penalty of one thousand dollars ($1,000) for each violation.

➔SECTION 3. A NEW SECTION OF KRS CHAPTER 6 IS CREATED TO READ AS FOLLOWS:

No information obtained from or by use of facial recognition technology as defined in Section 1 of this Act may be received in evidence in any legislative committee, task force, or other legislative body.

➔SECTION 4. A NEW SECTION OF KRS CHAPTER 13B IS CREATED TO READ AS FOLLOWS:

No information obtained from or by use of facial recognition technology as defined in Section 1 of this Act may be received in evidence in an administrative hearing.

➔SECTION 5. A NEW SECTION OF KRS CHAPTER 23A IS CREATED TO READ AS FOLLOWS:

No information obtained from or by use of facial recognition technology as defined in Section 1 of this Act may be received in evidence in any trial, hearing, or other proceeding.

➔SECTION 6. A NEW SECTION OF KRS CHAPTER 24A IS CREATED TO READ AS FOLLOWS:

No information obtained from or by use of facial recognition technology as defined in Section 1 of this Act may be received in evidence in any trial, hearing, or other proceeding.

➔SECTION 7. A NEW SECTION OF KRS CHAPTER 29A IS CREATED TO READ AS FOLLOWS:

No information obtained from or by use of facial recognition technology as defined in Section 1 of this Act may be received in evidence before a grand jury.

➔SECTION 8. A NEW SECTION OF THE KENTUCKY RULES OF

EVIDENCE IS CREATED TO READ AS FOLLOWS:

Evidence obtained by use of facial recognition technology, as defined in applicable statutes, is not admissible.