SENATE BILL NO. 397

INTRODUCED BY K. BOGNER, K. ZOLNIKOV, K. SULLIVAN, J. ESP, S. HINEBAUCH, S. FITZPATRICK, M. NOLAND, D. LENZ, S. MORIGEAU, J. ELLSWORTH, D. ZOLNIKOV

A BILL FOR AN ACT ENTITLED: “AN ACT ESTABLISHING THE FACIAL RECOGNITION FOR GOVERNMENT USE ACT; PROVIDING A PURPOSE; PROHIBITING THE USE OF CONTINUOUS FACIAL SURVEILLANCE; PROHIBITING THE USE OF FACIAL RECOGNITION TECHNOLOGY; PROVIDING EXEMPTIONS FOR LAW ENFORCEMENT; PROVIDING EXEMPTIONS UNDER CERTAIN CONDITIONS; PROVIDING FOR NOTICE REQUIREMENTS; PROVIDING FOR RETENTION AND DESTRUCTION REQUIREMENTS; PROVIDING FOR REPORTING REQUIREMENTS; PROVIDING FOR PENALTIES; PROVIDING DEFINITIONS; PROVIDING FOR A TRANSITION; AND PROVIDING AN IMMEDIATE EFFECTIVE DATE AND A RETROACTIVE APPLICABILITY DATE.”

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MONTANA:

NEW SECTION. **Section 1. Short title.** [Sections 1 through 12] may be cited as the "Facial Recognition for Government Use Act".

NEW SECTION. **Section 2. Purpose.** (1) Except as provided in subsection (2), the purpose of [sections 1 through 12] is to prohibit the use of facial recognition technology for continuous facial surveillance or facial identification by state and local government agencies and law enforcement agencies.

(2) It is the intent of the legislature to provide state and local government agencies the guidelines to use, or contract with third parties to use on their behalf, facial verification and to provide law enforcement agencies the ability to use facial recognition technology for investigations of serious crimes.

NEW SECTION. **Section 3. Definitions.** As used in [sections 1 through 12], unless the context clearly indicates otherwise, the following definitions apply:

(1) "Affirmative authorization" means an action that demonstrates the intentional decision by an

(5) [Sections 1 through 12] do not apply to a state or local government agency that uses facial verification in association with a federal agency to verify the identity of individuals presenting themselves for travel at an airport or other port.

NEW SECTION. **Section 9. Notice requirement -- policy and retention requirements for third-party vendors.** (1) On capturing an image of an individual when the individual interacts with a state or local government agency, the state or local government agency shall notify the individual that the individual's image may be used in conjunction with a facial recognition service.

(2) A third-party vendor contracted with a state or local government agency for the provision of a facial recognition service may not collect, capture, purchase, receive through trade, or otherwise obtain an individual's facial biometric data in the implementation of the service unless it first:

(a) informs the individual or the individual's legally authorized representative in writing that facial biometric data is being collected or stored;

(b) informs the individual or the individual's legally authorized representative in writing of the specific purpose and length of term for which facial biometric data is being collected, stored, and used; and

(c) receives written consent from the individual or the individual's legally authorized representative authorizing the collection, storage, and use of the individual's facial biometric data.

(3) A third-party vendor contracted with a state or local government agency for the provision of a facial recognition service shall provide the state or local government agency with a written privacy policy. The privacy policy must be designed and presented in a way that is easy to read and is understandable to an average consumer and must include the date the policy was last updated. A third-party vendor shall give notice of a privacy policy change to the state or local government agency within a reasonable period.

(4) (a) Except as provided in subsection (4)(b), a third-party vendor in possession of facial biometric data because of a contract with a state or local government agency for the provision of a facial recognition service shall develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying facial biometric data when the initial purpose for collecting or obtaining the data has been satisfied. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a third-party vendor in possession of facial biometric data shall comply with its established retention

schedule and destruction guidelines.

(b) A third-party vendor in possession of facial biometric data because of a contract with a state or local government agency for the provision of a facial recognition service may retain an individual's facial biometric data after the initial purpose for collecting or obtaining the data has been satisfied on the affirmative authorization of the individual. Facial biometric data retained because of affirmative authorization must be permanently destroyed within 1 year of the individual's last interaction with the third-party vendor.

(5) (a) A third-party vendor in possession of facial biometric data as a result of a contract with a state or local government agency for the provision of a facial recognition service shall develop a written information security policy establishing appropriate administrative, technical, and physical controls to establish and govern the acceptable use of the third-party vendor's information technology, including networks, applications, and databases, to protect the confidentiality, integrity, and availability of any facial biometric data.

(b) The security policy under subsection (5)(a) must include a provision that the facial biometric data collected under [sections 1 through 12] is stored within the territorial boundaries of the United States.

(6) A third-party vendor in possession of facial biometric data because of a contract with a state or local government agency for the provision of a facial recognition service may not give, sell, lease, or trade an individual's facial biometric data without affirmative authorization from the individual.

(7) A third-party vendor in possession of facial biometric data because of a contract with a state or local government agency for facial recognition services:

(a) shall store, transmit, and protect from unauthorized disclosure all facial biometric data collected and processed:

(i) using the reasonable standard of care within the third-party vendor's industry; and

(ii) in a manner that is the same as or more protective than the way the third-party vendor stores, transmits, and protects other personal information; and

(b) may not release facial biometric data to a federal or state agency without a valid warrant or court order issued by a court of competent jurisdiction.

(8) A state or local government agency that uses facial recognition technology without a third-party vendor must develop the same written privacy and retention policies outlined in this section as required by a third-party vendor, and must adhere to the same provisions for retention, destruction, and privacy as provided

in this section.

NEW SECTION. **Section 10. Meaningful human review -- policy.** A state or local government agency using a facial recognition service without a third-party vendor shall establish a policy that:

(1) ensures best quality results by following all guidance provided by the developer of the facial recognition service; and

(2) outlines training protocol for all individuals who operate a facial recognition service or who process personal data obtained from the use of a facial recognition service. The training must include but is not limited to coverage of:

(a) the capabilities and limitations of the facial recognition service;

(b) procedures to interpret and act on the output of the facial recognition service; and

(c) to the extent applicable, the meaningful human review requirement for decisions that produce legal effects concerning individuals.

NEW SECTION. **Section 11. Audit -- reporting.** (1) The criminal intelligence information section shall adopt an audit process to ensure that facial recognition technology is only used for legitimate law enforcement purposes, including audits of uses or requests made by law enforcement agencies.

(2) By September 1 of each year, in accordance with 5-11-210, the department of justice shall submit a report to the economic affairs interim committee and the law and justice interim committee containing all the following information based on data from the previous calendar year:

(a) the names of the law enforcement agencies and other entities requesting facial recognition services;

(b) the number of searches run;

(c) the offenses that the searches were used to investigate; and

(d) the number of arrests and convictions that resulted from the searches.

(3) (a) By June 30 of each year, a third-party vendor providing facial recognition services to a state agency because of a contract under [section 8] shall submit a report to the state agency containing all the following information based on data from the previous calendar year: