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:

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

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.

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

individual to opt into the retention of the individual's facial biometric data by a third-party vendor.

(2) "Another jurisdiction" means the federal government, the United States military, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, the United States Virgin Islands, Guam, American Samoa, a federally recognized Indian tribe, or a state other than Montana.

(3) "Continuous facial surveillance" means the monitoring of public places or third-party image sets using facial recognition technology for facial identification to match faces with a prepopulated list of face images. The term includes but is not limited to scanning stored video footage to identify faces in the stored data, real-time scanning of video surveillance to identify faces passing by the cameras, and passively monitoring video footage using facial recognition technology for general surveillance purposes without a particularized suspicion of a specific target.

(4) "Department" means the department of justice.

(5) "Digital driver's license" means a secure version of an individual's physical driver's license or identification card that is stored on the individual's mobile device.

(6) "Facial biometric data" means data derived from a measurement, pattern, contour, or other characteristic of an individual's face, either directly or from an image.

(7) (a) "Facial identification" means a computer system that, for the purpose of attempting to determine the identity of an unknown individual, uses an algorithm to compare the facial biometric data of an unknown individual derived from a photograph, video, or image to a database of photographs or images and associated facial biometric data in order to identify potential matches.

(b) The term does not include:

(i) a system used specifically to protect against unauthorized access to a particular location or an electronic device; or

(ii) a system a consumer uses for the consumer's private purposes.

(8) "Facial recognition service" or "facial recognition technology" means the use of facial identification or facial verification.

(9) "Facial verification" means the automated process of comparing an image or facial biometric data of a known individual to an image database, or to government documentation containing an image of the

known individual, to identify a potential match in pursuit of the individual's identity.

(10) "Law enforcement agency" means:

(a) an agency or officer of the state of Montana or of a political subdivision that is empowered by the laws of this state to conduct investigations or to make arrests; and

(b) an attorney, including the attorney general, who is authorized by the laws of this state to prosecute or to participate in the prosecution of a person who is arrested or who may be subject to a civil action related to or concerning an arrest.

(11) "Motor vehicle division" means the division within the department of justice authorized to issue driver's licenses.

(12) "Personal information" has the same meaning as in 30-14-1704.

(13) "Public building" means any building that the state or any political subdivision of the state maintains for the use of the public.

(14) "Public employee" means a person employed by a state or local government agency, including but not limited to a peace officer.

(15) "Public official" means a person elected or appointed to a public office that is part of a state or local government agency.

(16) "Public roads and highways of this state" has the same meaning as in 15-70-401.

(17) "Serious crime" means:

(a) a crime under the laws of this state that is a violation of 45-5-102, 45-5-103, 45-5-104, 45-5-106, 45-5-202, 45-5-207, 45-5-210, 45-5-212, 45-5-213, 45-5-220, 45-5-302, 45-5-303, 45-5-401, 45-5-503, 45-5-504(3), 45-5-508, 45-5-602, 45-5-603, 45-5-622, 45-5-625, 45-5-627, 45-5-628, 45-5-702, 45-5-703, 45-5-704, or 45-5-705; or

(b) a crime under the laws of another jurisdiction that is substantially similar to a crime under subsection (17)(a).

(18) "State or local government agency" means a state, county, or municipal government, a department, agency, or subdivision of a state, county, or municipal government, or any other entity identified in law as a public instrumentality. The term does not include a school district or law enforcement agency.

(19) "Vendor" has the same meaning as in 18-4-123.

Section 4. Prohibition of continuous facial surveillance. (1) A state or local government agency, law enforcement agency, public employee, or public official may not obtain, retain, possess, access, request, contract for, or use continuous facial surveillance.

(2) The use of facial recognition technology for facial verification, including any resulting data, may not be used to aid or assist in any type of continuous facial surveillance.

Section 5. Prohibition of facial recognition technology. (1) Except as provided in [sections 6 and 8], a state or local government agency, law enforcement agency, public employee, or public official may not:

(a) obtain, retain, possess, access, request, or use facial recognition technology or information derived from a search using facial recognition technology;

(b) enter into an agreement with a third-party vendor for any purpose listed in subsection (1)(a); or

(c) install or equip a continuous facial surveillance monitoring camera on public buildings or on public roads and highways of this state, except as provided in 46-5-117.

(2) The motor vehicle division may not establish a digital driver's license program that utilizes facial recognition technology without the consent of the legislature.

Section 6. Use of facial recognition technology by law enforcement -- when permitted -- restrictions on use -- warrant required. (1) The department of justice and local law enforcement agencies are authorized to use facial recognition technology for criminal investigations.

(2) The department of justice or a local law enforcement agency may perform a search using facial recognition technology and may obtain, retain, possess, access, or use the results of a search using facial recognition technology, as provided in subsection (3), for the purpose of:

(a) investigating a serious crime when there is probable cause to believe that an unidentified individual in an image has committed, is a victim of, or is a witness to a serious crime;

(b) assisting in the location or identification of a missing or endangered person; or

(c) assisting in the identification of a person who is deceased or believed to be deceased.

(3) Except as provided in subsection (5), a law enforcement agency shall obtain a warrant prior to

performing a search using facial recognition technology under subsection (2).

(4) A law enforcement agency shall obtain a court order authorizing the use of facial recognition technology for the sole purpose of locating or identifying a missing person or identifying a deceased person under subsections (2)(b) and (2)(c). A court may issue an ex parte order under this subsection if a law enforcement agency certifies and the court finds that the information to be obtained is likely relevant to locating or identifying a missing person or identifying a deceased person.

(5) (a) A law enforcement agency may perform a search under subsection (2) using facial recognition technology prior to the issuance of a warrant if there is an emergency posing an imminent threat to a person. If an emergency exists under this subsection (5)(a), the law enforcement agency shall obtain a warrant within 24 hours of the search.

(b) The use of facial recognition technology must terminate immediately if the application for a warrant under subsection (5)(a) is denied.

(6) A law enforcement agency may not use the results of facial recognition technology as the sole basis to establish probable cause in a criminal investigation. The results of the use of facial recognition technology may be used in conjunction with other information and evidence lawfully obtained by a law enforcement officer to establish probable cause in a criminal investigation.

(7) A law enforcement agency may not use facial recognition technology to identify an individual based on a sketch or other manually produced image.

(8) A law enforcement agency may not substantively manipulate an image for use with facial recognition technology in a manner not consistent with the facial recognition technology provider's intended use and training.

(9) When using facial recognition for identification of an individual, the department or local law enforcement shall employ meaningful human review prior to making an adverse final decision.

Section 7. Disclosure to criminal defendants. (1) A law enforcement agency or the department shall disclose the use of facial recognition technology on a criminal defendant to that defendant in a timely manner prior to trial.

(2) Discovery of an application, affidavit, or court order relating to the use of facial recognition and

any documents related to the use or request for use of facial recognition technology, if any, are subject to the provisions in Title 46, chapter 15.

(3) Data derived from the use of facial recognition technology in violation of [sections 1 through 12]:

(a) must be considered unlawfully obtained and, except as otherwise provided by law, must be deleted on discovery; and

(b) is inadmissible in evidence in a proceeding in or before a public official, department, regulatory body, court, or authority.

Section 8. Use of facial recognition technology by state and local government agencies -- when permitted -- restrictions on use -- exemption. (1) A state or local government agency may use, or contract with a third-party vendor for the use of, facial verification if the state or local government agency first provides a written use and privacy policy regarding facial recognition technology. The written policy must include, at a minimum:

(a) the specific purpose for facial verification by the state or local government agency;

(b) the length of term for which facial biometric data is being collected or stored; and

(c) notice that facial biometric data may not be collected on an individual without prior written consent by the individual.

(2) The state or local government agency must include an option for access to services without the use of facial verification.

(3) A third-party vendor who is contracted with a state or local government agency shall provide a copy of its written policies in accordance with [section 9] for use with the notice requirement outlined in subsection (1).

(4) A state or local government agency shall report the use of facial recognition technology pursuant to subsection (1) to the information technology board created in 2-15-1021.

(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.

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.

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.

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 June 30 of each year, a local law enforcement agency that utilized facial recognition technology shall submit a report to the criminal intelligence information section established in 44-5-501 containing all of the following information based on data from the previous calendar year:

(a) the number of facial recognition searches run;

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

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

(3) 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 information submitted to the department of justice pursuant to subsection (2);

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

(c) the number of searches run;

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

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

(4) (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:

(i) the number of warrants, subpoenas, or court orders received requesting facial recognition services; and

(ii) a summary of an audit completed by the third-party vendor.

(b) The state agency receiving the report from the third-party vendor shall submit a copy of the report to the economic affairs interim committee, the law and justice interim committee, and the information technology board created in 2-15-1021, by September 1 of each year, in accordance with 5-11-210.

Section 12. Penalty. (1) A violation of [sections 1 through 12] constitutes an injury and a person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in a court of competent jurisdiction to enforce [sections 1 through 12].

(2) A person who has been subjected to facial recognition technology in violation of [sections 1 through 12] or about whom information has been obtained, retained, accessed, or used in violation of [sections 1 through 12] may institute proceedings in a court of competent jurisdiction.

(3) A public employee or public official who, in the performance of their official duties, violates [sections 1 through 12] may be subject to disciplinary action, including but not limited to retraining, suspension, or termination, subject to the requirements of due process and of an applicable collective bargaining agreement.

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

(a) against an entity that negligently violates a provision of [sections 1 through 12], $1,000 or actual damages, whichever is greater;

(b) against an entity that intentionally or recklessly violates a provision of [sections 1 through 12], $5,000 or actual damages, whichever is greater;

(c) against an entity that negligently violates a provision of [sections 4 or 5], $5,000 or actual damages, whichever is greater;

(d) against an entity that intentionally or recklessly violates a provision of [sections 4 or 5], $10,000 or actual damages, whichever is greater;

(e) reasonable attorney fees and costs, including expert witness fees and other litigation expenses; and

(f) other relief, including an injunction, as the court may consider appropriate.

(5) The attorney general may bring an action to enforce [sections 1 through 12]. In an action brought by the attorney general, a violation of [sections 1 through 12] is subject to a civil penalty of $10,000 or actual damages, whichever is greater, for each violation.

(6) Nothing in this section limits the rights under state or federal law of a person injured or aggrieved by a violation of this section.

Section 13. Severability. If a part of [this act] is invalid, all valid parts that are severable from the invalid part remain in effect. If a part of [this act] is invalid in one or more of its applications, the part remains in effect in all valid applications that are severable from the invalid applications.

Section 14. Transition. A third-party vendor who has an enforced contract with the department of corrections, the department of justice, or the department of labor and industry as of [the effective date of this act] shall comply with the provisions of [this act] by January 1, 2024.

Section 15. Codification instruction. [Sections 1 through 12] are intended to be codified as a new chapter in Title 44, and the provisions of Title 44 apply to [sections 1 through 12].

Section 16. Effective date. [This act] is effective on passage and approval.

Section 17. Retroactive applicability. [This act] applies retroactively, within the meaning of 1-2-109, to contracts for third-party facial recognition services signed or renewed by the department of corrections, the department of justice, and the department of labor and industry as of January 1, 2022.

- END -

I hereby certify that the within bill,

SB 397, originated in the Senate.

_____

Secretary of the Senate

_____

President of the Senate

Signed this _____day

of_____, 2023.

_____

Speaker of the House

Signed this _____day

of_____, 2023.

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

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.