**** BILL NO. ****

INTRODUCED BY ****

BY REQUEST OF THE ****

A BILL FOR AN ACT ENTITLED: “AN ACT ESTABLISHING THE FACIAL RECOGNITION FOR GOVERNMENT USE ACT; PROVIDING A PURPOSE; PROVIDING DEFINITIONS; ESTABLISHING NOTICE OF INTENT; ESTABLISHING POLICY AND RETENTION REQUIREMENTS FOR THIRD-PARTY VENDORS; PROVIDING FOR WHEN MEANINGFUL HUMAN REVIEW IS REQUIRED; REQUIRING DISCLOSURE TO CRIMINAL DEFENDANTS; PROVIDING FOR RESTRICTIONS AND LIMITED ALLOWANCE OF FACIAL RECOGNITION SYSTEMS; REQUIRING A WARRANT FOR USE OF FACIAL RECOGNITION SYSTEMS BY LAW ENFORCEMENT; PROVIDING EXEMPTIONS; ESTABLISHING AUDIT AND REPORTING REQUIREMENTS; PROVIDING PENALTIES; PROVIDING A GRANDFATHER CLAUSE; AND PROVIDING AN EFFECTIVE DATE.”

WHEREAS, the 2021 Legislature passed House Joint Resolution 48, requesting an interim legislative study the use of facial recognition technology by state and local government agencies; and

WHEREAS, these studies were assigned to the Economic Affairs Interim Committee; and

WHEREAS, after 14 months of testimony and examination of data and information from all stakeholders, the Economic Affairs Interim Committee identified benefits and drawbacks to using facial recognition technology by state and local government agencies; and

WHEREAS, accordingly, the Economic Affairs Interim Committee recommends this bill to establish safeguards that will allow state and local government agencies to use facial recognition technology in a manner that benefits society while prohibiting uses that put civil liberties at risk.

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

NEW SECTION. **Section 1. Short title.** [Sections 1 through 10] may be cited as the "Facial Recognition for Government Use Act".

NEW SECTION. **Section 2. Purpose.** (1) The purpose of [this act] is to establish allowable uses of facial recognition technology by state and local government agencies.

(2) It is the intent of the legislature to provide state and local government agencies the ability to use facial recognition services for limited uses including fraud prevention, probation services, and for certain criminal investigations.

NEW SECTION. **Section 3. Definitions.** As used in [this act], unless the context clearly indicates otherwise, the following definitions apply:

(1) "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, federally recognized Indian tribes and each of the several states except Montana.

(2) "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.

(3) "Facial recognition comparison" means the process of comparing an image or facial biometric data to an image database.

(4) (a) "Facial recognition system" means a computer system that, for the purpose of attempting to determine the identity of an unknown individual, uses an algorithm to compare biometric data of the face of the unknown individual to facial biometric data of unknown individuals.

(b) "Facial recognition system" does not include;

(i) a system described in subsection (3)(a) that is available for use, free of charge, by the general public; or

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

(5) "Law enforcement agency" has the same meaning as in 44-11-303.

(6) "Legislative authority" means the respective city, county, or other local governmental agency's council, commission, or other body in which legislative powers are vested. For a state agency, "legislative authority" refers to the information technology board created in 2-15-1021.

(7) "Motor Vehicle Division" means the division within the department of justice authorized to issue driver's licenses.

(8) "Peace officer" has the same meaning as in 44-2-115.

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

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

(11) "Public official" means a person elected or appointed to a public office that is part of a department.

(12) "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, 45-5-210, 45-5-212, 45-5-213, 45-5-220, 45-5-302, 45-5-303, 45-5-503, 45-5-508, 45-5-625, 45-5-627, 45-5-628, 45-5-702, 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 (a).

(13) "State or local government agency" means a state, county, or municipal government or a department, agency, or subdivision thereof or any other entity identified in law as a public instrumentality, including, but not limited to, a law enforcement agency.

(14) "Vendor" has the same meaning as in 18-14-123.

NEW SECTION. **Section 4. Notice of intent -- policy and retention requirements for third-party vendors.** (1) A state or local government agency using, or contracting with a third-party vendor for, a facial recognition system must file with a legislative authority a notice of intent to use, or contract with a third-party vendor for, a facial recognition system and specify a purpose for which the technology is used.

(2) When capturing an image of an individual when the individual interacts with the 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 system.

(3) A third-party vendor in possession of facial biometric data must 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 such data has been satisfied or within 3 years

of the individual's last interaction with the third-party vendor, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a third-party vendor in possession of facial biometric data must comply with its established retention schedule and destruction guidelines.

(4) No third-party vendor contracted with a state or local government agency may collect, capture, purchase, receive through trade, or otherwise obtain an individual's facial biometric data 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 individual's legally authorized representative authorizing the collection, storage, and use of the individual's facial biometric data.

(5) No third-party vendor in possession of facial biometric data may sell, lease, trade, or otherwise profit from an individual's facial biometric data.

(6) A third-party vendor in possession of facial biometric data shall store, transmit, and protect from disclosure all facial biometric data:

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

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

NEW SECTION. **Section 5. Meaningful human review -- policy.** (1) A state or local government agency using facial recognition for identification of an individual shall employ meaningful human review prior to making final decisions based on such profiling where such final decisions produce legal effects concerning individuals or similarly significant effects concerning individuals.

(2) A state or local government agency using, or contracting with a third-party vendor for, a facial recognition system, must establish a policy that:

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

(b) outlines training protocol for all individuals who operate a facial recognition system or who

process personal data obtained from the use of a facial recognition system. The training must include, but not be limited to, coverage of:

(i) the capabilities and limitations of the facial recognition system;

(ii) procedures to interpret and act on the output of the facial recognition system; and

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

NEW SECTION. **Section 6. Disclosure to criminal defendants.** (1) A state or local government agency must disclose their use of a facial recognition system 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 facial recognition and any documents related to the use or request of facial recognition, if any, are subject to the Montana Code of Civil Procedure and the Montana Code of Criminal Procedure.

(3) Facial recognition data collected or derived in violation of [this act]:

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

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

NEW SECTION. **Section 7. Use of facial recognition systems -- restrictions on law enforcement use.** The following provisions govern the use of facial recognition systems by a state or local government agency or by a public employee or public official in the performance of their official duties.

(1) Except as provided in subsection (2), a state or local government agency, public employee or public official may not:

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

(b) Enter into an agreement with a third-party for the purpose of obtaining, retaining, possessing, accessing, or using, by or on behalf of a state or local government agency, public employee or public official, a

facial recognition system or information derived from a search of a facial recognition system; or

(c) issue a permit to enter into any other agreement that authorizes a third-party to obtain, retain, possess, access, or use a facial recognition system or information derived from a search of a facial recognition system.

(2) Except as provided in subsection (1), a law enforcement agency may request a search of a facial recognition system as provided in subsection (3) and may obtain, retain, possess, access, or use the results of a search of a facial recognition system, as provided in subsection (3), for the purposes of:

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

(b) assisting in the 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) The following provisions apply when a law enforcement agency requests a search of a facial recognition system under subsection (2):

(a) A request for a search of the facial recognition system within the state must be made to the criminal intelligence information section established in 44-5-501.

(b) A law enforcement agency must obtain a warrant prior to requesting a search of the facial recognition system under subsection (2)(a).

(c) A law enforcement agency must obtain a court order authorizing the use of the facial recognition system 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 (3)(c) if a law enforcement officer certifies and the court finds that the information likely to be obtained is relevant to locating or identifying a missing person, or identifying a deceased person.

(4) A state or local government agency may not apply a facial recognition system to any individual based on their religious, political, or social views or activities, participation in a particular noncriminal organization or lawful event, or actual or perceived race, ethnicity, citizenship, place of origin, immigration status, age, disability, sex, gender, gender identity, sexual orientation, or other characteristic protected by law. This subsection does not condone profiling including, but not limited to, predictive law enforcement tools.

(5) A state or local government agency may not use a facial recognition system to create a record

describing any individual's exercise of rights guaranteed by the First Amendment of the United States Constitution and by article II, section 7 of the state Constitution.

(6) A law enforcement agency may not use the results of a facial recognition system as the sole basis to establish probable cause in a criminal investigation. The results of a facial recognition system 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 a facial recognition system 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 in a facial recognition system in a manner not consistent with the facial recognition system provider's intended use and training.

NEW SECTION. **Section 8. Exemptions.** (1) This chapter does not apply to a state or local government agency that:

(a) is mandated to use a specific facial recognition system pursuant to a federal regulation or order, or that are undertaken through partnership with a federal agency to fulfill a congressional mandate; or

(b) uses a facial recognition system in association with a federal agency to verify the identity of individuals presenting themselves for travel at an airport or other port.

(2) A state or local government agency must report to a legislative authority the use of a facial recognition system pursuant to subsection (1).

NEW SECTION. **Section 9. Audit -- Reporting.** (1) The Montana State Police Fusion Center and any law enforcement agency using facial recognition services shall adopt an audit process to ensure that facial recognition is used only for legitimate law enforcement purposes, including audits of uses or requests made by law enforcement agencies or individual law enforcement officers.

(2) No later than September 1 of each year, the department of corrections, in conjunction with the criminal information intelligence center and law enforcement agencies that requested facial recognition comparison, shall submit a report to the economic affairs interim committee and law and justice interim

committee containing all the following information based on data from the previous calendar year:

(a) the number of searches run;

(b) the number of arrests and convictions that resulted from the searches;

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

(d) a list of audits that were completed by the criminal information intelligence center or a law enforcement agency and a summary of the audit results.

(3) (a) No later than June 30 of each year, any third-party vendor providing facial recognition services to a state or local government agency shall submit a report to the state or local government 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;

(ii) the statutory offense under investigation; and

(iii) a summary of any audit completed by the third-party vendor.

(b) The state or local government agency receiving the report from the third-party vendor must submit a copy of the report to the economic affairs interim committee and law and justice interim committee by September 1 each year.

NEW SECTION. **Section 10. Penalty.** (1) Any violation of [this act] constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in any court of competent jurisdiction to enforce [this act].

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

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

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

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

(b) against an entity that intentionally or recklessly violates a provision of [this act], liquidated damages of [$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.

(5) The attorney general may bring an action to enforce [this act]. In any action brought by the attorney general, a violation of [this act] is subject to a civil penalty of [$1,000] for each violation.

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

NEW SECTION. **Section 11. {standard} 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.

NEW SECTION. **Section 12. Grandfather clause.** Contracts for third-party facial recognition services held by the department of corrections, department of justice, and department of labor and industry as of January 1, 2022, are grandfathered in and are not subject to [this act] except any third-party vendors must comply with the provisions in [section 5] upon contract renewal.

NEW SECTION. **Section 13. Effective date.** [This act] is effective October 1, 2023.

- END -