**** 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; PROHIBITING THE USE OF FACIAL RECOGNITION BY STATE AND LOCAL GOVERNMENT AGENCIES; PROHIBITING THE PROCESSING OF FACIAL BIOMETRIC DATA BY STATE AND LOCAL GOVERNMENT AGENCIES; ESTABLISHING NOTICE OF INTENT; ESTABLISHING POLICY AND RETENTION REQUIREMENTS; REQUIRING DISCLOSURE OF PRIOR COLLECTION OF FACIAL BIOMETRIC DATA; REQUIRING DISCLOSURE TO CRIMINAL DEFENDANTS; PROVIDING FOR EXEMPTIONS; ESTABLISHING REPORTING REQUIREMENTS; PROVIDING FOR PENALTIES; AND PROVIDING AN IMMEDIATE EFFECTIVE DATE.”

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

WHEREAS, the study was assigned to the Economic Affairs Interim Committee; and

WHEREAS, after 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 school districts; and

WHEREAS, accordingly, the Economic Affairs Interim Committee recommends this bill to establish safeguards that restrict the use of facial recognition technology in a manner that safeguards the Montana Constitutional right of privacy by prohibiting the use of facial recognition technology that puts civil liberties at risk.

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

NEW SECTION. **Section 1. Short title.** [Sections 1 through 11] may be cited as the "Facial

Recognition for Government Use Act".

NEW SECTION. **Section 2. Purpose.** The purpose of [sections 1 through 11] is to prohibit the use of facial recognition technology and the processing of facial biometric data by state and local government agencies and school districts.

NEW SECTION. **Section 3. Definitions.** As used in [sections 1 through 11], unless the context clearly indicates otherwise, the following definitions apply:

(1) "Biometric data" means the personal data resulting from technical processing relating to the physical, psychological, or behavioral characteristics of a natural person, which allows or confirms that natural person's unique identification, such as but not limited to facial images or dactyloscopic data. Biometric data is personally identifiable information.

(2) "Data breach" means the unauthorized acquisition of covered information that compromises the security, integrity, or confidentiality of covered information.

(3) "Facial biometric data" means biometric data derived from a measurement, pattern, contour, or other characteristic of an individual's body part that occur above the shoulders of a natural person collected or derived from facial imaging, iris scans, ear scans, and images.

(4) "Facial identification" means recording effaced so that it can be searched for or recognized in the future, checking for matches in a database of already known faces or values representing those faces, searching for, or finding a particular face, processing measures in response to detecting a specific face.

(5) "Facial recognition" means recognizing a human face through technology. A facial recognition system uses biometrics to map facial features from a photograph or video.

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

(7) "Facial recognition technology" means an electronic system for enrolling, capturing, extracting, comparing, and matching an individual's geometric facial data to identify individuals in photos, videos, or in real-time. Facial recognition technology does not include the use of an automated or semi-automated process to redact a recording in order to protect the privacy of a subject depicted in the recording prior to release or

disclosure of the recording outside of the law-enforcement agency if the process does not generate or result in the retention of any biometric data or surveillance information.

(8) "Facial surveillance" means an automated or semi-automated process that assists in identifying or verifying an individual or in capturing information about an individual based on the physical characteristics of an individual's face.

(9) "Facial surveillance system" means any computer software application that performs facial surveillance or video cameras, still cameras, or other devices that has the capability of assisting in the facial identification of individuals.

(10) "Filing system" means any structured set of personal data accessible according to specific criteria, whether centralized, decentralized, or dispersed on a functional or geographical basis.

(11) "Iris scan" means a measure of the unique pattern of the colored circles in a person's eyes.

(12) "Law enforcement agency" means a police department of a city, village, or township, a sheriff's department, the department of state police, or any other governmental law enforcement agency in this state.

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

(14) "Personal data" means any information relating to an identified or identifiable natural person.

(15) "Personally identifiable information" means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Personally identifiable information is defined as information:

(a) that directly identifies an individual such as but not limited to name, address, social security number or other identifying number or code, telephone number, or e-mail address;

(b) by which an agency intends to identify specific individuals in conjunction with other data elements including a combination of gender, race, birth date, geographic indicator, and other descriptors; and

(c) information permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic, or other media.

(16) "Personal information" means information that may identify, relate to, describe, or reasonably link, directly or indirectly, with a particular individual or household.

(17) "Public employee" means a person employed by a state or local government agency or school district, including, but not limited to, a peace officer. The term includes a volunteer, contractor, or agent.

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

(19) "Sensitive data" means personal data of an individual such as religion, political opinions, sexual orientation, biometric and genetic data, and information that does not identify a person but can still be utilized to detect individual behavior patterns and may be used to track a matching group of individuals or a specific individual.

(20) "State or local government agency" means a state, county, municipal government, school district 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.

(21) "Third-party" means a natural or legal person, public authority, agency, agent, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

NEW SECTION. **Section 4. Prohibition of facial surveillance by a state and local government agency, public official, or public employee.** (1) A state or local government agency, public official, public employee may not:

(a) purchase or deploy facial recognition technology or purchase or use a private entity's deployment of facial recognition technology. For the purposes of this section, a statute that does not refer to facial recognition technology shall not be construed to provide express authorization.

(b) obtain, retain, possess, or access facial biometric data from a facial recognition service, facial surveillance system, or any other source that used facial recognition technology, database, or information derived from a search of a facial recognition system, database, or service;

(c) enter into an agreement with a third-party for the purpose of obtaining, retaining, possessing, accessing, processing facial biometric data or using facial recognition technology by or on behalf of a state or local government agency, public employee, public official, or third-party;

(d) enter into an agreement with a third-party authorizing the use or deployment of a facial surveillance system or other facial recognition technology;

(e) enter into an agreement that authorizes a private third-party or entity to obtain, retain, possess, access, or use facial biometric data, facial recognition technology, or information derived from a search using facial recognition technology;

(f) share, submit, or allow access to individual facial biometric data to a third-party except when required by federal statute or regulation;

(g) require the submission of facial biometric data to obtain a benefit or insurance coverage that is offered or required by state statute or regulation except for:

(i) photographs required for driver's licenses or state-issued identification and maintained by the motor vehicle division;

(ii) photographs collected of offenders by law enforcement as authorized by statute after arrest; and

(iii) photographs collected of offenders by the department of corrections.

(2) Facial biometric data submitted or collected under subsection (g) shall not be subject to facial recognition technology and must be kept confidential, not be disseminated or resold, except as required by 46-23-508(1)(b)(iv).

(3) Facial biometric data collected under subsection (4)(g)(ii) must be deleted and destroyed if the arrest does not result in a conviction.

NEW SECTION. **Section 5. Prohibition of processing of facial biometric data.** A state or local government agency, public official, public employee, or non-governmental agency that directly receives state funds shall not:

(1) process facial biometric data using facial recognition technology or other automated processes;

(2) provide facial biometric data for use, access, storage, or processing by a non-governmental entity or individual; or

(3) allow, agree to, or otherwise permit a private entity to collect facial biometric data.

NEW SECTION. **Section 6. Notice of intent -- policy and retention requirements.** (1) A third-party vendor or state or local government agency 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 1 year of the individual's last interaction with the third-party vendor, state or local government agency whichever occurs first.

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

(3) A third-party vendor or state or local government entity in possession of facial biometric data shall protect the data at rest, in motion, and data in transit, storage, transmission, and protect from disclosure all facial biometric data by the use of data encryption:

(a) using the reasonable standard of care within the data security 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.

(4) No third-party vendor contracted with a state or local government agency may store, collect, capture, purchase, receive through trade, or otherwise obtain an individual's facial biometric data and subject such data to facial recognition technology.

(5) A third-party vendor or state or local government agency in possession of facial biometric data shall notify individuals of the existence of facial biometric data in their possession, control, and the date of its destruction in accordance with subsection (1).

(6) (a) A third-party vendor or state or local government agency in possession of facial biometric data shall not share facial biometric data with any private entity or government agency without a proper warrant or court order.

(b) A warrant served upon a third-party vendor or state or local government agency in possession of facial biometric data shall be immediately forwarded to the state attorney general for review.

NEW SECTION. **Section 7. Disclosure of prior collection and use of facial biometric data and collection agreements -- notification of breach. (1)** A state or local government agency shall notify the public of prior use of facial recognition technology within 180 days of the effective date of this statute. Notification must include the following:

(a) the name of the facial recognition technology system, locations that the facial recognition

technology was deployed or used, and the purpose of the use of the technology; and

(b) the names and contact information of all entities who had access to, possession, processed or have retained possession, access, or control to the facial biometric data collected by the facial recognition technology system.

(2) A state or local government agency or third-party shall notify the public of potential or actual breaches of biometric data within 5 days of discovery of the potential or actual breach.

(3) The notification required in subsection (2) must contain the following information in plain language and using a 12-point font size or larger:

(a) name and contact information for the covered entity;

(b) types of sensitive information to include biometric data that was breached;

(c) date or estimated date range of the breach;

(d) date of the notice;

(e) whether notification was delayed due to law enforcement deeming that notification would interfere with an investigation;

(f) a general description of the breach;

(g) toll-free numbers and addresses for entities or agencies that manage social security numbers, driver's licenses, and related information if such information was breached.

NEW SECTION. **Section 8. Enforcement.** The following provisions apply to a violation of [sections 1 through 11] by a state or local government agency, public official, or public employee.

(1) Facial surveillance data collected or derived in violation of this section:

(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 court, public official, department, or regulatory authority.

(2) A state or local government agency, public official, or public employee may not apply a facial recognition system to identify any individual based on their religious, political, or social views or activities, participation in a particular 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.

(3) A state or local government agency, public official, public employee, school district, volunteer, or agent 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.

(4) A law enforcement agency may not use the results of a facial recognition system to establish probable cause in a criminal investigation.

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

NEW SECTION. **Section 9. 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] must be considered unlawfully obtained and, except as otherwise provided by law, must be deleted upon discovery and is inadmissible in any criminal proceeding.

NEW SECTION. **Section 10. Exemptions -- report required.** (1) [Sections 1 through 11] do not apply to a state or local government agency that:

(a) is mandated to use a facial recognition system pursuant to a mandatory federal regulation or statute; or

(b) uses a facial recognition system when required under subsection (1)(a) in association with a federal agency to verify the identity of individuals presenting themselves for travel at an airport or other port.

(2) The state or local government agency, school district, must report the use of a facial recognition technology system pursuant to this part to the economic affairs interim committee by June 1 each year. This part does not authorize the use of facial recognition technology.

(3) The report required in subsection (2) must contain all the following information based on data from the previous calendar year:

(a) date the facial recognition technology system was installed and the date the system operation ceased;

(b) the authority, statute, or regulation that authorized the facial recognition technology was deployed or used;

(c) number of individuals subjected to facial surveillance, collection of facial biometric data;

(d) the location that facial recognition technology was deployed or used;

(e) the purpose of the use, deployment, or installation of facial recognition technology or facial surveillance systems;

(f) the entities who have access to the facial biometric data collected or processed by the facial recognition technology system;

(g) the number and disposition of all facial biometric data collected by the facial recognition system and processed or stored and the number of records destroyed in accordance with subsection (1);

(h) the number of warrants and court orders, subject of the warrant, date received and data and database accessed per a warrant or court order received by a third-party vendor, state and local government, public official, public employee, school district, volunteer, or agent in possession of facial biometric data;

(i) the date of all biometric data breaches that resulted in the exposure in excess of twenty-five biometric records;

(j) the steps taken to secure the biometric data from future breaches and the methods employed in breaching the data security;

(k) the steps taken to permanently destroy and delete facial biometric data; and

(l) projected completion of deletion and destruction of facial biometric data.

NEW SECTION. **Section 11. Penalty.** (1) Any violation of [sections 1 through 11] 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 [sections 1 through 11].

(2) Any person who has been subjected to facial recognition in violation of [sections 1 through 11], or about whom the information has been obtain, retained, accessed, or used in violation of [sections 1 through 11], 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 [sections 1 through 11] 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 vendor as defined in 18-14-123 or other third-party operating in partnership, under license, agreement, with a state or local government agency, public official, public employee, school district, shall not collect, store, distribute, transfer, access, process, facial biometric data or subject users of electronic supplied by the state or local government agency, public official, public employee, or school district for use in education of individuals to facial recognition technology, facial surveillance, or biometric data collection.

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

(a) against an entity that negligently violates a provision of [sections 1 through 11], [$1,000] or actual damages, whichever is greater;

(b) against an entity that intentionally or recklessly violates a provision of [sections 1 through 11], [$5,000], or actual damages, whichever is greater;

(c) against a vendor or entity that intentionally or negligently violates subsection (4), damages equal to [10%] of the vendor or entity's annual world-wide revenue;

(d) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses;

(e) other relief, including an injunction, as the court may deem appropriate.

(6) The attorney general may bring an action to enforce [sections 1 through 11]. In any action brought by the attorney general, a violation of [sections 1 through 11] is subject to a civil penalty of [$10,000] or [15%] of the entity's annual world-wide revenue, whichever is greater, for each violation.

(7) 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 12. {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 13. {standard} Effective date.** [This act] is effective on passage and approval.

- END -