1   SENATE BILL NO. 397

2   INTRODUCED BY K. BOGNER, K. ZOLNIKOV, K. SULLIVAN, J. ESP, S. HINEBAUCH, S. FITZPATRICK, M.

3   NOLAND, D. LENZ, S. MORIGEAU, J. ELLSWORTH, D. ZOLNIKOV

4

5   A BILL FOR AN ACT ENTITLED: "AN ACT ESTABLISHING THE FACIAL RECOGNITION FOR

6   GOVERNMENT USE ACT; PROVIDING A PURPOSE; PROHIBITING THE USE OF CONTINUOUS FACIAL

7   SURVEILLANCE; PROHIBITING THE USE OF FACIAL RECOGNITION TECHNOLOGY; PROVIDING

8   EXEMPTIONS FOR LAW ENFORCEMENT; PROVIDING EXEMPTIONS UNDER CERTAIN CONDITIONS;

9   PROVIDING FOR NOTICE REQUIREMENTS; PROVIDING FOR RETENTION AND DESTRUCTION

10   REQUIREMENTS; PROVIDING FOR REPORTING REQUIREMENTS; PROVIDING FOR PENALTIES;

11   PROVIDING DEFINITIONS; PROVIDING FOR A TRANSITION; AND PROVIDING AN IMMEDIATE

12   EFFECTIVE DATE AND A RETROACTIVE APPLICABILITY DATE."

13

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

15

16   NEW SECTION. **Section 1.   Short title.** [Sections 1 through 12] may be cited as the "Facial

17   Recognition for Government Use Act".

18

19   NEW SECTION. **Section 2.   Purpose.** (1) Except as provided in subsection (2), the purpose of

20   [sections 1 through 12] is to prohibit the use of facial recognition technology for continuous facial surveillance or

21   facial identification by state and local government agencies and law enforcement agencies.

22   (2)   It is the intent of the legislature to provide state and local government agencies the guidelines

23   to use, or contract with third parties to use on their behalf, facial verification and to provide law enforcement

24   agencies the ability to use facial recognition technology for investigations of serious crimes.

25

26   NEW SECTION. **Section 3.   Definitions.** As used in [sections 1 through 12], unless the context

27   clearly indicates otherwise, the following definitions apply:

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

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

3   (2)   "Another jurisdiction" means the federal government, the United States military, the District of

4   Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, the United

5   States Virgin Islands, Guam, American Samoa, a federally recognized Indian tribe, or a state other than

6   Montana.

7   (3)   "Continuous facial surveillance" means the generalized monitoring of public places or third-

8   party image sets using facial recognition technology for facial identification to match faces with a prepopulated

9   list of face images. The term includes but is not limited to scanning stored video footage to identify faces in the

10   stored data, real-time scanning of video surveillance to identify faces passing by the cameras, and passively

11   monitoring video footage using facial recognition technology for general surveillance purposes without a

12   particularized suspicion of a specific target.

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

14   (5)   "Digital driver's license" means a secure version of an individual's physical driver's license or

15   identification card that is stored on the individual's mobile device.

16   (6)   "Facial biometric data" means data derived from a measurement, pattern, contour, or other

17   characteristic of an individual's face, either directly or from an image.

18   (7)   (a) "Facial identification" means a computer system that, for the purpose of attempting to

19   determine the identity of an unknown individual, uses an algorithm to compare the facial biometric data of an

20   unknown individual derived from a photograph, video, or image to a database of photographs or images and

21   associated facial biometric data in order to identify potential matches.

22   (b)   The term does not include:

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

24   electronic device; or

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

26   (8)   "Facial recognition service" or "facial recognition technology" means the use of facial

27   identification or facial verification.

Legislative
Services
Division

1   (9)   "Facial verification" means the automated process of comparing an image or facial biometric

2   data of a known individual to an image database, or to government documentation containing an image of the

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

4   (10)   "Law enforcement agency" means:

5   (a)   an agency or officer of the state of Montana or of a political subdivision that is empowered by

6   the laws of this state to conduct investigations or to make arrests; and

7   (b)   an attorney, including the attorney general, who is authorized by the laws of this state to

8   prosecute or to participate in the prosecution of a person who is arrested or who may be subject to a civil action

9   related to or concerning an arrest.

10   (11)   "Motor vehicle division" means the division within the department of justice authorized to issue

11   driver's licenses.

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

13   (13)   "Public building" means any building that the state or any political subdivision of the state

14   maintains for the use of the public.

15   (14)   "Public employee" means a person employed by a state or local government agency, including

16   but not limited to a peace officer.

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

18   local government agency.

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

20   (17)   "Serious crime" means:

21   (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-

22   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-

23   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-

24   704, or 45-5-705; or

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

26   subsection (17)(a).

27   (18)   "State or local government agency" means a state, county, or municipal government, a

1   department, agency, or subdivision of a state, county, or municipal government, or any other entity identified in

2   law as a public instrumentality. The term does not include a school district or law enforcement agency.

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

4

5   NEW SECTION. **Section 4.   Prohibition of continuous facial surveillance.** (1) A state or local

6   government agency, law enforcement agency, public employee, or public official may not obtain, retain,

7   possess, access, request, contract for, or use continuous facial surveillance.

8   (2)   The use of facial recognition technology for facial verification, including any resulting data, may

9   not be used to aid or assist in any type of continuous facial surveillance.

10

11   NEW SECTION. **Section 5.   Prohibition of facial recognition technology.** (1) Except as provided in

12   [sections 6 and 8], a state or local government agency, law enforcement agency, public employee, or public

13   official may not:

14   (a)   obtain, retain, possess, access, request, or use facial recognition technology or information

15   derived from a search using facial recognition technology;

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

17   (c)   install or equip a continuous facial surveillance monitoring camera on public buildings or on

18   public roads and highways of this state, except as provided in 46-5-117.

19   (2)   The motor vehicle division may not establish a digital driver's license program that utilizes facial

20   recognition technology without the consent of the legislature.

21

22   NEW SECTION. **Section 6.   Use of facial recognition technology by law enforcement -- when**

23   **permitted -- restrictions on use -- warrant required.** (1) The department of justice is the only state or local

24   government agency authorized to use facial recognition technology for criminal investigations. A request from a

25   law enforcement agency for a search using facial recognition technology must be made to the criminal

26   intelligence information section established in 44-5-501.

27   (2)   A law enforcement agency may request a search using facial recognition technology and may

1   obtain, retain, possess, access, or use the results of a search using facial recognition technology, as provided

2   in subsection (3), for the purpose of:

3   (a)   investigating a serious crime when there is probable cause to believe that an unidentified

4   individual in an image has committed, is a victim of, or is a witness to a serious crime;

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

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

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

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

9   (4)   A law enforcement agency shall obtain a court order authorizing the use of facial recognition

10   technology for the sole purpose of locating or identifying a missing person or identifying a deceased person

11   under subsections (2)(b) and (2)(c). A court may issue an ex parte order under this subsection if a law

12   enforcement agency certifies and the court finds that the information to be obtained is likely relevant to locating

13   or identifying a missing person or identifying a deceased person.

14   (5)   (a) A law enforcement agency may submit a request for a search under subsection (2) using

15   facial recognition technology prior to the issuance of a warrant if there is an emergency posing an imminent

16   threat to a person. If an emergency exists under this subsection (5)(a), the law enforcement agency shall obtain

17   a warrant within 24 hours of the request and submit the warrant to the criminal intelligence information section.

18   (b)   The use of facial recognition technology must terminate immediately if the application for a

19   warrant under subsection (5)(a) is denied.

20   (6)   A law enforcement agency may not use the results of facial recognition technology as the sole

21   basis to establish probable cause in a criminal investigation. The results of the use of facial recognition

22   technology may be used in conjunction with other information and evidence lawfully obtained by a law

23   enforcement officer to establish probable cause in a criminal investigation.

24   (7)   A law enforcement agency may not use facial recognition technology to identify an individual

25   based on a sketch or other manually produced image.

26   (8)   A law enforcement agency may not substantively manipulate an image for use with facial

27   recognition technology in a manner not consistent with the facial recognition technology provider's intended use

Legislative
Services
Division

1   and training.

2   (9)   When using facial recognition for identification of an individual, the department shall employ

3   meaningful human review prior to making an adverse final decision.

4

5   NEW SECTION. **Section 7.   Disclosure to criminal defendants.** (1) A law enforcement agency or

6   the department shall disclose the use of facial recognition technology on a criminal defendant to that defendant

7   in a timely manner prior to trial.

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

9   any documents related to the use or request for use of facial recognition technology, if any, are subject to the

10   provisions in Title 46, chapter 15.

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

12   12]:

13   (a)   must be considered unlawfully obtained and, except as otherwise provided by law, must be

14   deleted on discovery; and

15   (b)   is inadmissible in evidence in a proceeding in or before a public official, department, regulatory

16   body, or authority.

17

18   NEW SECTION. **Section 8.   Use of facial recognition technology by state and local government**

19   **agencies -- when permitted -- restrictions on use -- exemption.** (1) A state or local government agency may

20   use, or contract with a third-party vendor for the use of, facial verification if the state or local government

21   agency first provides a written use and privacy policy regarding facial recognition technology. The written policy

22   must include, at a minimum:

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

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

25   (c)   notice that facial biometric data may not be collected on an individual without prior written

26   consent by the individual.

27   (2)   The state or local government agency must include an option for access to services without the

1   use of facial verification.

2   (3)   A third-party vendor who is contracted with a state or local government agency shall provide a

3   copy of its written policies in accordance with [section 9] for use with the notice requirement outlined in

4   subsection (1).

5   (4)   A state or local government agency shall report the use of facial recognition technology

6   pursuant to subsection (1) to the information technology board created in 2-15-1021.

7   (5)   [Sections 1 through 12] do not apply to a state or local government agency that uses facial

8   verification in association with a federal agency to verify the identity of individuals presenting themselves for

9   travel at an airport or other port.

10

11   NEW SECTION. **Section 9.   Notice requirement -- policy and retention requirements for third-**

12   **party vendors.** (1) On capturing an image of an individual when the individual interacts with a state or local

13   government agency, the state or local government agency shall notify the individual that the individual's image

14   may be used in conjunction with a facial recognition service.

15   (2)   A third-party vendor contracted with a state or local government agency for the provision of a

16   facial recognition service may not collect, capture, purchase, receive through trade, or otherwise obtain an

17   individual's facial biometric data in the implementation of the service unless it first:

18   (a)   informs the individual or the individual's legally authorized representative in writing that facial

19   biometric data is being collected or stored;

20   (b)   informs the individual or the individual's legally authorized representative in writing of the

21   specific purpose and length of term for which facial biometric data is being collected, stored, and used; and

22   (c)   receives written consent from the individual or the individual's legally authorized representative

23   authorizing the collection, storage, and use of the individual's facial biometric data.

24   (3)   A third-party vendor contracted with a state or local government agency for the provision of a

25   facial recognition service shall provide the state or local government agency with a written privacy policy. The

26   privacy policy must be designed and presented in a way that is easy to read and is understandable to an

27   average consumer and must include the date the policy was last updated. A third-party vendor shall give notice

Legislative
Services
Division

1   of a privacy policy change to the state or local government agency within a reasonable period.

2   (4)   (a) Except as provided in subsection (4)(b), a third-party vendor in possession of facial

3   biometric data because of a contract with a state or local government agency for the provision of a facial

4   recognition service shall develop a written policy, made available to the public, establishing a retention

5   schedule and guidelines for permanently destroying facial biometric data when the initial purpose for collecting

6   or obtaining the data has been satisfied. Absent a valid warrant or subpoena issued by a court of competent

7   jurisdiction, a third-party vendor in possession of facial biometric data shall comply with its established retention

8   schedule and destruction guidelines.

9   (b)   A third-party vendor in possession of facial biometric data because of a contract with a state or

10   local government agency for the provision of a facial recognition service may retain an individual's facial

11   biometric data after the initial purpose for collecting or obtaining the data has been satisfied on the affirmative

12   authorization of the individual. Facial biometric data retained because of affirmative authorization must be

13   permanently destroyed within 1 year of the individual's last interaction with the third-party vendor.

14   (5)   A third-party vendor in possession of facial biometric data as a result of a contract with a state

15   or local government agency for the provision of a facial recognition service shall develop a written information

16   security policy establishing appropriate administrative, technical, and physical controls to establish and govern

17   the acceptable use of the third-party vendor's information technology, including networks, applications, and

18   databases, to protect the confidentiality, integrity, and availability of any facial biometric data.

19   (6)   A third-party vendor in possession of facial biometric data because of a contract with a state or

20   local government agency for the provision of a facial recognition service may not give, sell, lease, or trade an

21   individual's facial biometric data without affirmative authorization from the individual.

22   (7)   A third-party vendor in possession of facial biometric data because of a contract with a state or

23   local government agency for facial recognition services:

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

25   and processed:

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

27   (ii)   in a manner that is the same as or more protective than the way the third-party vendor stores,

1   transmits, and protects other personal information; and

2   (b)   may not release facial biometric data to a federal or state agency without a valid warrant or

3   court order issued by a court of competent jurisdiction.

4   (8)   A state or local government agency that uses facial recognition technology without a third-party

5   vendor must develop the same written privacy and retention policies outlined in this section as required by a

6   third-party vendor, and must adhere to the same provisions for retention, destruction, and privacy as provided

7   in this section.

8

9   NEW SECTION. **Section 10.   Meaningful human review -- policy.** A state or local government

10   agency using a facial recognition service without a third-party vendor shall establish a policy that:

11   (1)   ensures best quality results by following all guidance provided by the developer of the facial

12   recognition service; and

13   (2)   outlines training protocol for all individuals who operate a facial recognition service or who

14   process personal data obtained from the use of a facial recognition service. The training must include but is not

15   limited to coverage of:

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

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

18   (c)   to the extent applicable, the meaningful human review requirement for decisions that produce

19   legal effects concerning individuals.

20

21   NEW SECTION. **Section 11.   Audit -- reporting.** (1) The criminal intelligence information section

22   shall adopt an audit process to ensure that facial recognition technology is only used for legitimate law

23   enforcement purposes, including audits of uses or requests made by law enforcement agencies.

24   (2)   By September 1 of each year, in accordance with 5-11-210, the department of justice shall

25   submit a report to the economic affairs interim committee and the law and justice interim committee containing

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

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

1   services;

2   (b)   the number of searches run;

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

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

5   (3)   (a) By June 30 of each year, a third-party vendor providing facial recognition services to a state

6   agency because of a contract under [section 8] shall submit a report to the state agency containing all the

7   following information based on data from the previous calendar year:

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

9   services; and

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

11   (b)   The state agency receiving the report from the third-party vendor shall submit a copy of the

12   report to the economic affairs interim committee, the law and justice interim committee, and the information

13   technology board created in 2-15-1021, by September 1 of each year, in accordance with 5-11-210.

14

15   NEW SECTION. **Section 12.   Penalty.** (1) A violation of [sections 1 through 12] constitutes an injury

16   and a person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in a court of

17   competent jurisdiction to enforce [sections 1 through 12].

18   (2)   A person who has been subjected to facial recognition technology in violation of [sections 1

19   through 12] or about whom information has been obtained, retained, accessed, or used in violation of [sections

20   1 through 12] may institute proceedings in a court of competent jurisdiction.

21   (3)   A public employee or public official who, in the performance of their official duties, violates

22   [sections 1 through 12] may be subject to disciplinary action, including but not limited to retraining, suspension,

23   or termination, subject to the requirements of due process and of an applicable collective bargaining

24   agreement.

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

26   (a)   against an entity that negligently violates a provision of [sections 1 through 12], $1,000 or

27   actual damages, whichever is greater;

Legislative
Services
Division

1   (b)   against an entity that intentionally or recklessly violates a provision of [sections 1 through 12],

2     $5,000 or actual damages, whichever is greater;

3   (c)   against an entity that negligently violates a provision of [sections 4 or 5], $5,000 or actual

4   damages, whichever is greater;

5   (d)   against an entity that intentionally or recklessly violates a provision of [sections 4 or 5], $10,000

6   or actual damages, whichever is greater;

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

8   expenses; and

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

10   (5)   The attorney general may bring an action to enforce [sections 1 through 12]. In an action

11   brought by the attorney general, a violation of [sections 1 through 12] is subject to a civil penalty of $10,000 or

12   actual damages, whichever is greater, for each violation.

13   (6)   Nothing in this section limits the rights under state or federal law of a person injured or

14   aggrieved by a violation of this section.

15

16   NEW SECTION. **Section 13.   Severability.** If a part of [this act] is invalid, all valid parts that are

17   severable from the invalid part remain in effect. If a part of [this act] is invalid in one or more of its applications,

18   the part remains in effect in all valid applications that are severable from the invalid applications.

19

20   NEW SECTION. **Section 14.   Transition.** A third-party vendor who has an enforced contract with the

21   department of corrections, the department of justice, or the department of labor and industry as of [the effective

22   date of this act] shall comply with the provisions of [this act] by January 1, 2024.

23

24   NEW SECTION. **Section 15.   Codification instruction.** [Sections 1 through 12] are intended to be

25   codified as a new chapter in Title 44, and the provisions of Title 44 apply to [sections 1 through 12].

26

27   NEW SECTION. **Section 16.   Effective date.** [This act] is effective on passage and approval.

1

2   NEW SECTION. **Section 17.   Retroactive applicability.** [This act] applies retroactively, within the

3   meaning of 1-2-109, to contracts for third-party facial recognition services signed or renewed by the department

4   of corrections, the department of justice, and the department of labor and industry as of January 1, 2022.

5   - END -