Montana Coalition for Safety and Justice
1633 Main Street Ste A173
Billings, Montana 59105

June 7, 2022

Erin Sullivan
Lead Staff
Economic Affairs Interim Committee
P.O. Box 201706
Helena, Montana 1706
erin.sullivan@mt.gov

RE: HJ48 Draft Facial Recognition Bill

Dear Ms. Sullivan,

I have attached a draft of a bill that addresses facial recognition use in Montana by Government and private entities. The draft also contains a list of definitions that are generally used when addressing privacy and regulating the use of an individual's personally identifiable information or biometrics.

The bill is drafted to create a modular approach to privacy law in Montana where each section can be edited or adjusted as the statute area evolves to face new concerns and new technology.

Please forward us to those concerned and I hope that this will be helpful to the committee and the drafters of potential bills for the committee. If questions arise, please feel free to contact me.

Respectfully

Steve Cape
sc-policy@c4sj.org
(406) 284-1050

Draft Facial Recognition Bill

Economic Affairs Interim Committee -2022

New Section – Definitions

Biometric Data: 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.

Biometrics: All information or data that is subjected or processed.

Biometric Identifier: Is defined as a characteristic, whether biological, behavioral, or both, that enables automated recognition of an individual, including but not limited to D.N.A., hand geometry, palm print, iris scan, facial imaging, voice, gait, or other characteristics that are biological, anatomical or behavioral that may be used or identification of an individual that consists of distinguishing, repeatable biometric features that may be extracted for the purpose of identification of a natural person.

Binding Corporate Rules: Means personal data protection policies which are adhered to by a controller or processor doing business, offering services, information or products in the State for transfers or a set of transfers of personal data to a controller or processor individually, as agent, or within a group of undertakings, or group of enterprises engaged in a joint activity that contains or is connected to Personal Data of residents of Montana.

Business: means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for profit ,financial benefit of its shareholders or owners, a party, committee, association, fund or other organization organized and operated primarily for the purpose of directly or indirectly accepting contributions or making expenditures, or both for a tax exempt function under state or federal law and any entity controlled by or is a subsidiary of.

Department of Motor Vehicles: has the same meaning as in MCA _____

Commissioned Data Processing: Commissioned data processing applies when a company (controller) commissions an external service provider (contractor) to process, analyze or store personal data in an instruction-bound manner.

Consent: Means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Controller: Means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by State law.

Cross-Border Processing: Means processing of personal data which takes place in the context of the activities of establishments in the State of Montana, other State or States, or foreign countries of a controller or processor where the controller or processor is established in more than one State.

i. by electronic means' means that the service or product is sent initially and received at its destination by means of electronic equipment for the processing, including digital compression, and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means.

ii. at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request.

Data At Rest: means inactive data that is stored physically in any digital form

Data In Transit: data that is traveling over a network or networks.

Data Processor: A data processor is any natural or legal person, public authority, agency or other body which processes data on behalf of the controller.

Data Controller: A natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personally Identifiable Information. The controller or the specific criteria for its nomination may be provided State law or regulation.

Department:

Any division of state or local government to include law enforcement agencies, committees and groups that act under color of law

Enterprise: Means a natural or legal person engaged in an economic activity, irrespective of its legal form, including sole proprietorships, partnerships, Limited Liability Companies, Limited Liability Partnerships, Corporations or associations regularly engaged in an economic activity.

Facial Identification: 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 were measures in response to detecting a particular face.

Facial Recognition Data : Biometric Data derived from facial imaging, photo, or imaging of body parts that occur above the shoulders of a natural person.

Facial Recognition: Recognizing a human face through technology. A facial recognition system uses biometrics to map facial features from a photograph or video.

Facial Surveillance: Means an automated or semiautomated 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.

Facial Surveillance System: means any computer software application that performs facial surveillance or video cameras, still cameras, or other device that has the capability of assisting in facial identification of individuals.

Filing System: Means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

Genetic Data: Means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Health Data: Means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Identifiable Natural Person: Is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

International Organization: Means an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries and the agreement is recognized by the United States or the State of Montana by action of the Legislature.

Iris Scan: Iris scanning measures the unique patterns in irises, the colored circles in people's eyes2

Law Enforcement Agency: has the same meaning as in MCA _____.

Personal Data: means any information relating to an identified or identifiable natural person.

Personal Information: Information that may identify, relate to, describe, or reasonably link, directly or indirectly, with a particular individual or household.

Personally Identifiable Information

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. Further, PII is defined as information:

(i) that directly identifies an individual such as but not limited to; name, address, social security number or other identifying number or code, telephone number, email address, etc.) or

(ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors.

(iii) 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.

Personal Data Breach: Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Private Entity:
An individual, association, club, business and defined as a business under this title or other entity or group.

Processor: means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

Processing: Means: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Profiling: means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyses or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

Pseudonymization: Means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Public Employee: Means an employee of the state of Montana and any individual who salary or other renumeration source is directly funded by taxes imposed upon individuals by any entity authorized to do so by statute or regulation.

Public Official: Means a person elected or appointed to public office, public employee, or agent of a public official or public employee.

Recipient: Means a natural or legal person, public authority, agency, or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with State law shall not be regarded as recipients; the processing of those data by those public authorities shall follow the applicable data protection laws according to the purposes of the processing.

Representative: Means a natural or legal person who, designated by the controller or processor in writing pursuant State Law represents the controller or processor with regard to their respective obligations under State or Federal Law

Restriction of Processing: Means the marking of stored personal data with the aim of limiting their processing in the future.

Sensitive Data: 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.

Serious Crime: A serious crime is defined as acts that are violations of Montana Code Annotated 45-5-302, 45-5-303, 45-5-502, 45-5-503, 45-5-508, 45-5-603 45-5-625, 45-5-627, 45-5-702, 45-5-703, and Federal Statues 18 U.S.C. 1581, 18 U.S.C 1584

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.

Framework - Facial Recognition

FACIAL SURVEILANCE

New Section 1 – Facial Recognition by Government

Use Of Facial Surveillance by Department, Public Official, Public Employee.

1. A Department, public employee or public official shall not except as described in Section b,
   a. Obtain, or retain, possess, access, request or use a facial recognition service or a facial surveillance system or information derived from a search of a facial recognition system, database, or service, or
   b. Enter into an agreement with third party for the purpose of obtaining, retaining, possessing, accessing or using, by or on behalf of a government agency, department, public employee, public official or third party a facial surveillance system or information derived from a search of a facial surveillance system or
   c. Issue a permit to enter into an agreement that authorizes a private third party or entity to obtain, retain, possess, access, or use facial data, facial surveillance system or information derived from a search of a facial surveillance system.
   d. Require the submission of biometric data to obtain a benefit, or insurance coverage that is offered or required by State statute or regulation.
      i. This section does not apply to photographs required for driver's licenses or state issued identification.
      ii. This section does not apply to the requirement to provide identification for participating in an election process.

2. A government agency, department, public employee, or public official may request a search of a facial recognition database or system in compliance with section c for the purposes of:
   a. Investigating a serious crime where there is probable cause to believe that an unidentified individual in an image has committed the serious crime.
   b. Assisting in the identification of a person who is deceased.
   c. Assisting in the identification of a missing or endangered person who is incapacitated and unable to provide personal information necessary to identify the individual.

3. Requirements necessary to authorize a request a search of a facial recognition database or facial surveillance system by a government agency, department, public employee, or public official.
   a. A request for a search of a facial recognition database or facial recognition surveillance system under b(1) shall be made in compliance with M.C.A. 46-5-221.
   b. A request for a search of a facial recognition database or surveillance system for the purpose of identification of an individual who is deceased or incapacitated may be

authorized by a Court having jurisdiction sufficient to issue a search warrant under M.C.A. 46-5-221.

New Section – 2 Enforcement Government Official

1. The following provisions apply to a violation of this section by a Department or public employee or public official acting in the performance of their official duties or agents thereof.
2. 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 in or before any court, public official, department, regulatory body or authority.
3. A person whose facial recognition data has been obtained in violation of this section may bring an action in court in this state against the Department, public employee, public official, or agents
4. A person is facial recognition data has been obtained in violation of this section may bring an action in a court in this state against any department, public employee, public official, and/or their agents having possession, custody or control of facial surveillance data in violation of this section and may seek injunctive, declaratory relief and or a writ of mandamus and
5. A person whose facial recognitions been obtained in violation of this section may bring a monetary claim in any court in this state against any department, public employee, public official, and/or their agents having possession, custody, or control of facial surveillance data in violation of this section or obtained facial recognition data in violation of this section.
6. The person aggrieved shall be entitled to damages in the amount of $1,000 per incident.
    a. For the purposes of calculating damages under this section an incident shall be defined as a single search or image.
7. A public employee or public official who, in the performance of their official duties violates this section shall be subject to disciplinary action, including but not limited to retraining, suspension or termination, subject to the requirements of due process and any applicable collective bargaining agreement.
8. Nothing in this subsection limits the rights under state or federal law of the person injured or aggrieved by a violation of this section

New Section – 3 Biometric Data Use by Private Entity

1. A private entity shall not employ, use, contract for or otherwise access a biometric database including a facial database or facial surveillance system; except
    a. Business security entrance system to control access to high security areas, data or data systems, and.
    b. Individual has consented in writing to the use of facial recognition and,

i. Consent is valid when the individual was fully informed as to proposed use, third party access, processing, security and right to delete the individual's biometric data in writing.
ii. Individuals under 18 must have parental consent and such consent shall be in writing and such writing shall be separate in form and conform with the requirements of section 1(b).
It is is is here should be your

2. This section does not apply to businesses or other private entities that collect or process protected health information governed by the privacy, security, and breach notification rules established pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPPA) and the Health Information Technology for Economic and Clinical Health Act (HITECH)

3. A private entity shall safeguard biometric data under its control, process, or possession, and
   a. May not sell, lease, or otherwise disclose the biometric identifier to another person unless:
   b. The indi is is to be is true jurisdiction the easy relief was his this there is 6 8006 vidual consents to the disclosure for identification purposes in the event of the individual's disappearance or death;
   c. The disclosure completes a financial transaction that the individual requested or authorized;
   d. The disclosure is required or permitted by a federal statute,
   e. The disclosure is made by or to a law enforcement agency for a law enforcement purpose in response to a warrant;
   f. Shall store, transmit, and protect from disclosure the biometric identifier using reasonable care and such data is encrypted during transfer and at rest.
   g. Shall destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires, except as provided by Subsection 2(c).
   h. If a biometric identifier of an individual captured for a commercial purpose is used in connection with an instrument or document that is required by State or Federal statute to be maintained for a period longer than the period prescribed by Subsection (2)(c), the person who possesses the biometric identifier shall destroy the biometric identifier no later than the first anniversary of the date the instrument or document is no longer required to be maintained by law.
   i. If a biometric identifier captured for a commercial purpose has been collected for security purposes by a private entity, the purpose for collecting the identifier is presumed to expire on termination of the employment relationship,
      i. The business who possesses the biometric identifier shall destroy the biometric identifier no later than 30 days after the termination of the employment relationship

j. A private entity who violates this section is subject to a civil penalty of not less than $1,000 or more than $25,000 for each violation.
k. Nothing in this subsection limits the rights under state or federal law of the person injured or aggrieved by a violation of this section.
l. This section does not apply to voiceprint data retained by a financial institution or an affiliate of a financial institution, as those terms are defined by 15 U.S.C. Section 6809 .

4. A private entity may use biometric identifiers to allow secure User access to personal electronic devices that are owned by or operated by a specific user where the individual has;
   a. Consented in writing to the use of biometric identifiers,
      i. Consent is valid when the individual was fully informed as to use, third party access, processing, security and right to delete the individual's biometric data in a separate writing.
      ii. Individuals under 13 must consent in writing and have parental consent and
      iii. such consent shall be in writing and such writing shall be separate in form.

5. Privately Collected Biometric Information
   a. Biometric Information shall not be collected for entry, storage, processing, packaging, sales, marketing, or other activity that the entity either directly or indirectly receives a commercial benefit.
   b. Biometric information shall not be obtained, collected from third party sources unless prior individual consent is obtained
   c. Biometric information collected by a private entity shall be defined as Personally Identifiable Information.
   d. Biometric Information shall not be shared, processed, transferred accessed by a third party unless specific consent in writing is obtained by each processor. Such consent shall comply with the requirements of Section a(1).
   e. The Individual shall have the right to limit, deny or refuse consent for each processor, data controller, data processor.
   f. An individual shall have the right to have their biometric data permanently deleted from all systems or each individual system used by a specified processor, data processor, data controller and controller.
      i. Deletion shall be competed within 30 days of receipt of a written request by an individual.
      ii. Receipt of a deletion request shall be deemed to occur.
         a. 3 calendar days from the date of mailing using the United States Postal Service if recipient is located with the United States and its territories.

b. 10 calendar days if the recipient is located outside of the United States and territories.
c. 2 calendar days if the request is sent by e-mail or other electronic means using the named recipient's deletion request system.
d. 1 calendar day after personal service in the manner described in M.C.A. 39-3-508(2).

6. Individual Control of Biometric Information
    a. An individual shall have the right to limit access, processing, storage, use, transfer, and sale of their biometric information, and
    b. Consent in writing shall be required for each processor, of biometric information prior to accessing, processing, or storing of biometric information.
        i. Consent is not required for storage or processing when the biometric information is stored, accessed and processed on the device and cannot be accessed except for the individual user of the device.
        ii. The consent must inform the individual of their right to data deletion and give instructions on requesting such deletion.

New Section – 4 Enforcement Private Entity

1. The following provisions apply to a violation of this section by a private entity.
2. 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 in or before any public official, department, regulatory body, or authority.
3. A person whose facial recognition data has been obtained, processed, accessed, or collected in violation of this section may bring an action in court in this state against the entity and agents
4. Facial recognition data has been obtained in violation of this section may bring an action in a court in this state against an entity and their agents having possession, custody, access, or control of facial surveillance data obtained in violation of this section and may seek injunctive, declaratory and or a writ of mandamus and
5. A person whose biometric identifiers, facial data been obtained in violation of this section may bring a monetary claim in any court in this state against an entity and their agents having possession, custody access or control of facial surveillance data in violation of this section or obtained facial recognition data in violation of this section.
6. The person aggrieved shall be assumed to have been damaged in an amount of no less than $1,000 per incident.
    a. For the purposes of calculating damages under this section an incident shall be defined as a single search or image.

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