HOUSE BILL NO. 572

INTRODUCED BY B. BENNETT

A BILL FOR AN ACT ENTITLED: "AN ACT CREATING THE MONTANA RIGHT TO KNOW ACT; PROVIDING DEFINITIONS; REQUIRING ENTITIES TO ACCOUNT FOR DISCLOSURES OF INFORMATION; PROVIDING AN INDIVIDUAL WITH ACCESS TO PERSONAL INFORMATION COLLECTED BY OTHER ENTITIES; PROVIDING EXCEPTIONS TO DISCLOSURE; AND PROVIDING PENALTIES."

WHEREAS, the collection, sale, and trade of personal information frequently occurs without an individual's knowledge or consent; and

WHEREAS, the increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information; and

WHEREAS, all individuals have a right of privacy protected by Article II, section 10, of the Montana constitution, which states that the right of individual privacy is essential to the well-being of a free society and "shall not be infringed without the showing of a compelling state interest"; and

WHEREAS, to protect Montanans from exploitation, it is necessary to inform individuals of when and to whom their personal information has been disclosed.

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

NEW SECTION. **Section 1. Short title.** [Sections 1 through 8] be cited as the "Montana Right to Know Act".

NEW SECTION. **Section 2. Legislative purpose.** (1) The purpose of [sections 1 through 8] is to inform Montanans of when and to whom their personal information has been disclosed.

(2) The requirements of [sections 1 through 8] apply to all entities that provide services, software, or products to Montana residents, process personal information of data subjects who are Montana residents, or conduct business in the state of Montana.

NEW SECTION. **Section 3. Definitions.** As used in [sections 1 through 8], the following definitions

apply:

(1) "Agency" means every state office, officer, department, division, bureau, board, commission, or other state or local agency.

(2) "Business" means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or of any other country or the parent or the subsidiary of a financial institution. The term includes an entity that disposes of records.

(3) "Communication" means disclosure of personal information either through transmission of the data to the recipient or through the recipient inspecting or retrieving personal information held by the controller.

(4) "Controller" means any person collecting, processing, using, or disclosing personal information or commissioning others to collect, process, use, or disclose personal information.

(5) "Data subject" means the individual to whom personal information relates.

(6) "Disclose" means to disclose, release, transfer, disseminate, or otherwise communicate all or any part of any record orally, in writing, or by electronic or any other means to any person or entity.

(7) (a) "Entity" includes every business, government, and agency.

(b) The term does not include natural persons.

(8) "Hand-held communications device" means a device that is capable of providing mobile telecommunications services and that is designed to be carried by the end user. This term includes cell phones, smart phones, tablets, and other devices.

(9) "Individual" means a natural person.

(10) "Maintain" means to maintain, acquire, use, or disclose.

(11) "Mobile telecommunications services" means commercial mobile radio service, as defined in 47 CFR 20.3.

(12) "Person" means any individual, entity, or agency.

(13) "Personal information" includes the following types of information that may be potentially associated with an individual:

(a) medical records, including records of health conditions, symptoms, treatment, diagnoses, laboratory test information and results, and any information derived from this information;

(b) prescription information, including drug names, dosage, frequency, amounts, dates and times of

pickup, and any information derived from this information;

(c) shopping and purchase records, including descriptions of items purchased, the location of purchases, the dates and times of purchases, the price and amounts of purchases, any product return dates, times, locations, and other derived information, and ammunition purchase records, including caliber, brand, price, and amount;

(d) the individual's location, obtained using a hand-held communications device carried by the individual, a GPS tracking device, a radio tracking device, a radio frequency identification tag, an automated license plate reader, or facial recognition software;

(e) social security number, driver's license number, state identification card number, or tribal identification card number;

(f) web search terms, browser history, and information derived from this information; and

(g) passwords for personal e-mail, internet, and application accounts not including cryptographic hashes of passwords, such as those commonly used for login authentication.

(14) "Processing" means the storage, modification, communication, and erasure of personal information.

(15) "Processor" means any entity involved in collection, processing, or use of personal information on the controller's behalf for the purposes stated by the controller.

(16) (a) "Record" means any medium, regardless of the physical form, on which personal information is recorded or preserved by any means, including in written or spoken words, graphically or visually depicted, printed, or electromagnetically transmitted.

(b) The term does not include publicly available data containing information that an individual has voluntarily consented to have publicly disseminated or listed.

(17) "Storage" means the entry, recording, or preservation of personal data on a storage medium so that the data can be processed or used again.

(18) "System of records" means one or more records that pertain to one or more individuals, that are maintained by any entity, and that contain personal information.

(19) "Use" means any utilization of personal information other than processing.

NEW SECTION. **Section 4. Accounting of disclosure.** (1) Each entity shall keep an accurate accounting of each disclosure of a record of information potentially associated with an individual.

(2) The accounting of disclosure must include the name, title, and business address of the person or entity to whom the disclosure was made, the date of disclosure, and an accurate description of or reference to

each record disclosed.

(3) Each entity shall retain the accounting of disclosure made pursuant to subsection (1) for at least 3 years after the disclosure for which the accounting is made.

(4) Nothing in this section may be construed to require retention of the original documents for a 3-year period if the entity is otherwise able to comply with the requirements of this section.

(5) For purposes of this section, "potentially associated with an individual" means that it may be possible to identify the data subject related to a specific piece of information. Collections of information associated with the same anonymous identifier, such as a number or code, are considered to be potentially associated with an individual.

NEW SECTION. **Section 5. Access.** (1) Each individual has the right to inquire and be notified as to whether an entity maintains or has maintained a record about the individual. In addition, each individual has the right to inquire and receive a copy of records maintained about the individual and any corresponding accounting of disclosure pursuant to [section 4]. Entities shall take reasonable steps to assist individuals in making their requests sufficiently specific.

(2) Entities shall designate a point of contact responsible for receiving and responding to requests pursuant to subsection (1). Entities shall publish the title and contact information for this point of contact, including business address and phone number, as well as the procedures to be followed to gain access to records and the accounting of disclosure. Entities shall take reasonable steps to ensure that this information is available to data subjects without undue effort on the part of individuals seeking to make requests pursuant to subsection (1).

(3) Upon receipt of a request pursuant to subsection (1), an entity shall provide an accurate and complete response to the individual within 60 days of the entity's receipt of the request. In implementing the provisions of this section, an entity may specify in its rules or regulations reasonable times, places, and requirements for identifying an individual who requests access and for disclosing the contents of a record or the accounting of disclosure.

(4) Except as otherwise provided in [sections 1 through 8], each entity shall, within 60 days of receiving a request from a data subject, permit the data subject upon proper identification to inspect all the personal information regarding that individual, as well as the accounting of disclosures made pursuant to [section 4], and have an exact copy made of all or any portion of the information. Failure to respond within this time limit is considered a denial.

(5) Within 60 days of the entity's receipt of a data subject's request, the entity shall permit another person of the data subject's own choosing to inspect all the personal information in the record relating to the data subject and the accounting of disclosures made pursuant to [section 4] and have an exact copy made of all or any portion of the information. The entity may require the data subject to furnish a written statement authorizing disclosure of the data subject's record to another person.

(6) The entity shall present information in the record and the accounting of disclosures in a form reasonably comprehensible to the general public.

(7) Whenever an entity is unable to access a record by reference to name only or when access by name only would impose an unreasonable administrative burden, the entity may require the data subject to submit other identifying information to facilitate access to the record.

(8) When an individual is entitled under [sections 1 through 8] to gain access to the information in a record containing personal information or the accounting of disclosure the information or a true copy of the record must be made available to the individual at a location near the residence of the individual or by mail, whenever reasonable.

(9) Each entity may establish fees to be charged to an individual for making copies of a record and the accounting of disclosure as provided in 2-6-110.

(10) The data subject's right to information under this section may not be excluded or restricted by contract.

(11) If the personal information of the data subject is stored in a system of records shared by several entities and the data subject is unable to ascertain the controller of a record, the data subject may approach any of the entities. An entity is required to forward the data subject's request to the controller of the record. The data subject must be informed of the forwarding of the request and of the controller of the record.

(12) This section applies to the rights of a data subject to whom personal information pertains and not to the authority or right of any other person or entity to obtain this information.

NEW SECTION. **Section 6. Exceptions.** (1) [Sections 1 through 8] may not be construed to require an entity to disclose personal information to the data subject if the information:

(a) is compiled for the purpose of identifying individual criminal offenders and alleged offenders and consists only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status;

(b) is compiled for the purpose of a criminal investigation of suspected criminal activities, including reports of informants and investigators, and is associated with an identifiable individual;

(c) is contained in any record that could identify an individual and is compiled at any stage of the process of enforcement of the criminal laws, from the arrest or indictment stage through release from supervision and including the process of extradition or the exercise of executive clemency;

(d) is maintained for the purpose of an investigation of an individual's fitness for licensure or public employment, of a grievance or complaint, or of a suspected civil offense, as long as the information is withheld only so that it does not compromise the investigation. The identities of individuals who provided information for the investigation may be withheld.

(e) may compromise the objectivity or fairness of a competitive examination for appointment or promotion, to determine fitness for licensure, or to determine scholastic aptitude;

(f) pertains to the physical or psychological condition of the data subject and the entity determines that disclosure would be detrimental to the data subject. The information must be disclosed, upon the data subject's written authorization, to a licensed medical practitioner or psychologist designated by the individual.

(g) relates to the settlement of claims for work-related illnesses or injuries and is maintained exclusively by the state compensation insurance fund; or

(h) is required by statute to be withheld from the data subject.

(2) This section may not be construed to deny a data subject access to information relating to the data subject if access is allowed by another law of this state.

(3) (a) Except as provided in subsection (3)(c), if the entity determines that requested information is exempt from access, the entity shall inform the data subject in writing of the entity's finding that disclosure is not required by law.

(b) Except as provided in subsection (3)(c), each entity shall conduct a review of its determination that particular information is exempt from access within 30 days from the receipt of a request by a data subject directly affected by the determination and inform the data subject in writing of the findings of the review. The review must be conducted by the head of the entity or an official specifically designated by the head of the entity.

(c) If the entity believes that compliance with subsection (3)(a) would seriously interfere with attempts to apprehend persons who are wanted for committing a crime or with attempts to prevent the commission of a crime or would endanger the life of an informant or other person submitting information contained in the record, the entity may petition the presiding judge of the superior court of the county in which the record is maintained

to issue an ex parte order authorizing the entity to respond to the individual by stating that no record is maintained. All proceedings before the court must be in camera. If the presiding judge finds that there are reasonable grounds to believe that compliance with subsection (3)(a) will seriously interfere with attempts to apprehend persons who are wanted for committing a crime or with attempts to prevent the commission of a crime or will endanger the life of an informant or other person submitting information contained in the record, the judge shall issue an order authorizing the entity to respond to the individual by stating that no record is maintained by the entity. The order may not be issued for longer than 30 days but may be renewed at 30-day intervals. If a request pursuant to this section is received after the expiration of the order, the entity shall either respond pursuant to subsection (3)(a) or seek a new order pursuant to this section.

(4) In disclosing information contained in a record to an individual, an entity may not disclose any personal information relating to another individual that may be contained in the record. To comply with this section, an entity shall, in disclosing information, delete from disclosure any information as is necessary. This section may not be construed as authorizing the withholding of identities of sources except as provided in subsection (1).

NEW SECTION. **Section 7. Contracted entities.** (1) A controller may contract with a processor to collect, process, use, or disclose records containing personal information on the collector's behalf. The controller is responsible for ensuring compliance with [sections 1 through 8].

(2) The processor shall provide the controller with the title, business address, and telephone number of the entity official who is responsible for the system of records for any future correspondence regarding the personal information being disclosed under the provisions of the contract.

(3) Within 60 days of receipt of a written request, the controller shall provide the data subject with the names of all processors who have received the data subject's personal information, as well as the title, business address, and telephone number of each corresponding entity official who is responsible for the system of records.

(4) Data subjects have the right to request information regarding their personal information directly from processors, and the processor shall comply in accordance with [sections 4 and 5].

NEW SECTION. **Section 8. Violations.** (1) A person who willfully, as defined in 1-1-204, requests or obtains any record containing personal information from an entity under false pretenses, bribery, theft, or misrepresentation of identity, purpose of use, or entitlement is guilty of a misdemeanor and shall be fined not

more than $5,000, imprisoned for not more than 1 year, or both.

(2) A data subject may bring a civil action against an entity whenever an entity:

(a) refuses to comply with a data subject's lawful request for information pursuant to [section 5];

(b) fails to accurately and completely maintain any accounting of disclosure concerning a data subject;

(c) fails to comply with any other provision of [sections 1 through 8] or any administrative rule adopted to implement [sections 1 through 8] in a manner that has an adverse effect on a data subject.

(3) (a) In any suit brought under the provisions of this section:

(i) the court may enjoin the entity from withholding the records and order the production to the complainant of any entity records improperly withheld from the complainant. The court may examine the contents of any entity records in camera to determine whether the records or any portion of the records may be withheld as being exempt from the data subject's right of access. The burden is on the entity to sustain its denial of access to the data subject.

(ii) the court may assess against an entity reasonable attorney fees and costs incurred in any suit under this section in which the complainant has prevailed. A party may be considered to have prevailed even though a party does not prevail on all issues or against all parties.

(b) Any entity that fails to comply with any provision of [sections 1 through 8] may be enjoined by any court of competent jurisdiction. The court may make any order or judgment as may be necessary to prevent any practices by an entity that violate [sections 1 through 8].

(4) Actions for injunction under this section may be prosecuted by the attorney general or any county attorney in this state, whether the action is brought upon the attorney general's or county attorney's own complaint, by a member of the general public, or by any individual acting on an individual's own behalf.

(5) In any suit brought under the provisions of subsection (3), the entity is liable to the individual in an amount equal to the sum of:

(a) compensatory and special damages sustained by the individual, including damages for emotional distress; and

(b) the costs of the action together with reasonable attorney fees as determined by the court.

(6) An action to enforce the provisions of [sections 1 through 8] may be brought within 2 years from the date on which the cause of action arises in any court in the county in which the complainant resides or has a principal place of business or where the defendant's records are located. An exception exists when a defendant materially and willfully misrepresents any information required under [sections 1 through 8] to be disclosed to a

data subject who is the subject of the information and the information misrepresented is material to the establishment of the defendant's liability to that data subject under [sections 1 through 8]. The action may be brought at any time within 2 years after discovery by the complainant of the misrepresentation.

(7) The rights and remedies set forth in [sections 1 through 8] are nonexclusive and are in addition to those rights and remedies that are available under any other provision of law.

NEW SECTION. **Section 9. Codification instruction.** [Sections 1 through 8] are intended to be codified as an integral part of Title 30, chapter 14, and the provisions of Title 30, chapter 14, apply to [sections 1 through 8].

- END -