LEGISLATURE OF THE STATE OF IDAHO
Sixty-fifth Legislature Second Regular Session - 2020

IN THE HOUSE OF REPRESENTATIVES

HOUSE BILL NO. 492

BY ENVIRONMENT, ENERGY AND TECHNOLOGY COMMITTEE

AN ACT

RELATING TO FACIAL RECOGNITION TECHNOLOGY; AMENDING TITLE 73, IDAHO CODE, BY THE ADDITION OF A NEW CHAPTER 5, TITLE 73, IDAHO CODE, TO PROVIDE A SHORT TITLE, TO PROVIDE LEGISLATIVE INTENT, TO DEFINE TERMS, TO PROVIDE APPLICABILITY, TO PROVIDE FOR CONTROLLER AND PROCESSOR OBLIGATIONS, TO ESTABLISH CERTAIN INDIVIDUAL RIGHTS REGARDING FACIAL RECOGNITION, TO PROVIDE CERTAIN LIMITATIONS, TO PROVIDE FOR LIABILITY, TO PROVIDE FOR ENFORCEMENT, TO PROVIDE FOR AN ACCOUNTABILITY REPORT, TO PROVIDE FOR CERTAIN ANNUAL REPORTING, TO PROVIDE FOR MEANINGFUL HUMAN REVIEW BY AGENCIES, TO PROVIDE FOR OPERATIONAL TESTING BY AGENCIES, TO PROVIDE FOR CERTAIN TRAINING OF AGENCY PERSONNEL, TO ESTABLISH PROVISIONS REGARDING ONGOING SURVEILLANCE, TO PROVIDE FOR DUE PROCESS PROTECTIONS, AND TO PROVIDE FOR PREEMPTION; AND PROVIDING SEVERABILITY.

Be It Enacted by the Legislature of the State of Idaho:

SECTION 1. That Title 73, Idaho Code, be, and the same is hereby amended by the addition thereto of a NEW CHAPTER, to be known and designated as Chapter 5, Title 73, Idaho Code, and to read as follows:

CHAPTER 5
FACIAL RECOGNITION TECHNOLOGY

73-501. SHORT TITLE. This chapter shall be known and may be cited as the "Facial Recognition Technology Act."

73-502. DECLARATION OF POLICY. The legislature finds that:

(1) Use of facial recognition services by the private sector and by state and local government agencies can present risks to privacy, democratic freedoms, and civil liberties that should be considered and addressed.

(2) Facial recognition technology can also be used in a variety of beneficial ways, such as improving security, providing individuals with efficient identification experiences, locating missing or incapacitated persons, identifying victims of crime, and keeping the public safe.

(3) Accordingly, this legislation is required to establish safeguards that will allow industry and government to use facial recognition services in ways that benefit society while prohibiting uses that threaten our privacy, our democratic freedoms, and our civil liberties.

73-503. DEFINITIONS. As used in this chapter:

(1) "Accountability report" means a report developed in accordance with section 73-510, Idaho Code.

(2) "Agency" means a state or local government agency in the state of Idaho.

(3) "Consent" means a clear affirmative act signifying a freely given, specific, informed, and unambiguous indication of an individual's agreement to the processing of personal data relating to the individual, such as by a written statement, including by electronic means or other clear affirmative action.

(4) "Controller" means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data. An agency is not a controller.

(5) "Enroll," "enrolled," or "enrolling" means the process by which a facial recognition service creates a facial template from one (1) or more images of an individual and adds the facial template to a gallery used by the facial recognition service for recognition or persistent tracking of individuals. Such term also includes the act of adding an existing facial template directly into a gallery used by a facial recognition service.

(6) "Facial recognition service" means technology that analyzes facial features and is used for recognition or persistent tracking of individuals in still or video images.

(7) "Facial template" means the machine-interpretable pattern of facial features that is extracted from one (1) or more images of an individual by a facial recognition service.

(8) "Identified or identifiable natural person" means a person who can be readily identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, specific geolocation data, or an online identifier.

(9) "Meaningful human review" means review or oversight by one (1) or more individuals who are trained in accordance with section 73-512, Idaho Code, and who have the authority to alter the decision under review.

(10) "Ongoing surveillance" means tracking the physical movements of a specified individual through one (1) or more public places over time, whether in real time or through application of a facial recognition service to historical records. Such term does not include a single recognition or attempted recognition of an individual if no attempt is made to subsequently track that individual's movement over time after such individual has been recognized.

(11) "Persistent tracking" means the use of a facial recognition service by a controller or an agency to track the movements of an individual on a persistent basis without using the facial recognition service for recognition of that individual. Such tracking becomes persistent as soon as:

(a) The controller or agency maintains the facial template or unique identifier that permits the tracking for more than forty-eight (48) hours after that template or identifier is first created; or

(b) The controller or agency links the data created by the facial recognition service to any other data including without limitation purchase or payment data, such that the individual who has been tracked is identified or identifiable.

(12) "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. Personal data does not include de-identified data or publicly available information. For purposes of this chapter, "publicly available information" means

information that is lawfully made available from federal, state, or local government records.

(13) "Process" or "processing" means any collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(14) "Processor" means a natural or legal person that processes personal data on behalf of a controller. An agency is not a processor.

(15) "Recognition" means the use of a facial recognition service by a controller or an agency to predict whether:

(a) An unknown individual matches any individual who has been enrolled in a gallery used by the facial recognition service; or

(b) An unknown individual matches a specific individual who has been enrolled in a gallery used by the facial recognition service.

(16) "Security or safety purpose" means physical security, safety, fraud prevention, or asset protection.

(17) "Serious criminal offense" means any felony under chapter 1, title 18, Idaho Code, or an offense pursuant to 18 U.S.C. 2516.

73-504. APPLICABILITY. The provisions of sections 73-505 through 73-509, Idaho Code, shall apply to legal entities that conduct business in Idaho or produce products or services that are targeted to residents of Idaho.

73-505. CONTROLLER AND PROCESSOR OBLIGATIONS. (1) Processors that provide facial recognition services shall make available an application programming interface or other technical capability, chosen by the processor, to enable controllers or third parties to conduct legitimate, independent, and reasonable tests of those facial recognition services for accuracy and unfair performance differences across distinct subpopulations. Such subpopulations may be defined by race, skin tone, ethnicity, gender, age, disability status, or other protected characteristic that is objectively determinable or self-identified by the individuals portrayed in the testing dataset. If the results of such independent testing identify materially unfair performance differences across subpopulations and those results are disclosed directly to the processor who, acting reasonably, determines that the methodology and results of that testing are valid, then the processor must develop and implement a plan to mitigate the identified performance differences. Nothing in this subsection prevents a processor from prohibiting the use of his facial recognition service by a competitor for competitive purposes.

(2) Processors that provide facial recognition services must provide documentation that includes general information that:

(a) Explains the capabilities and limitations of the services in plain language; and

(b) Enables testing of the services in accordance with this section.

(3) Processors that provide facial recognition services must prohibit, in the contract by which the controller is permitted to use the facial recognition service, the use of such facial recognition services by controllers to unlawfully discriminate under federal or state law against individuals or groups of individuals.

(4) Controllers must provide a conspicuous and contextually appropriate notice whenever a facial recognition service is deployed in a physical premises open to the public that includes, at a minimum, the following:

(a) The purpose or purposes for which the facial recognition service is deployed; and

(b) Information about where individuals can obtain additional information about the facial recognition service, including but not limited to a link to any applicable online notice, terms, or policy that provides information about where and how individuals can exercise any rights that they have with respect to the facial recognition service.

(5) Controllers must obtain consent from an individual prior to enrolling an image or a facial template of that individual in a facial recognition service used in a physical premises open to the public.

(6) Except as provided in subsection (5) of this section, controllers may enroll an image or a facial template of an individual in a facial recognition service for a security or safety purpose without first obtaining consent from that individual provided that each of the following requirements is met:

(a) The controller must hold a reasonable suspicion, based on a specific incident, that the individual has engaged in criminal activity, which includes but is not limited to shoplifting, fraud, stalking, or domestic violence;

(b) Any database used by a facial recognition service for recognition, verification, or persistent tracking of individuals for a security or safety purpose must be used solely for that purpose and maintained separately from any other databases maintained by the controller;

(c) The controller must review any such database used by his facial recognition service no less than biannually to remove facial templates of individuals in respect to whom the controller no longer holds a reasonable suspicion that they have engaged in criminal activity or that are more than three (3) years old; and

(d) The controller must establish an internal process whereby individuals may correct or challenge the decision to enroll the image of an individual in a facial recognition service for a security or safety purpose.

(7) Controllers using a facial recognition service to make decisions that produce legal effects concerning individuals or similarly significant effects concerning individuals must ensure that those decisions are subject to meaningful human review. Decisions that produce legal effects concerning individuals or similarly significant effects concerning individuals shall include but not be limited to denial of consequential services or support, such as financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, and access to basic necessities such as food and water.

(8) Prior to deploying a facial recognition service in the context in which it will be used, controllers must test the facial recognition service in operational conditions. Controllers must take commercially reasonable steps to ensure best quality results in operational conditions by following all reasonable guidance provided by the developer of the facial recognition service.

(9) Controllers using a facial recognition service must conduct periodic training of all people who operate a facial recognition service or who process personal data obtained from the use of facial recognition services. Such training shall include but not be limited to coverage of:

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

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

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

(10) Controllers shall not knowingly disclose personal data obtained from a facial recognition service to a law enforcement agency except when such disclosure is:

(a) Pursuant to the consent of the individual to whom the personal data relates;

(b) Required by federal, state, or local law in response to a court order, court-ordered warrant, subpoena, or summons issued by a judicial officer, or a grand jury subpoena;

(c) Upon a good faith belief by the controller that the disclosure is necessary to prevent or respond to an emergency involving danger of death or serious physical injury to any person; or

(d) To the national center for missing and exploited children, in connection with a report submitted pursuant to 18 U.S.C. 2258A.

73-506. INDIVIDUAL RIGHTS. (1) Individuals may exercise the rights set forth in this section by submitting a request, at any time, to a controller specifying which rights the individual wishes to exercise. Except as provided in this chapter, the controller must comply with a request to exercise the rights pursuant to this section. The processor shall assist the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the controller's obligation to respond to individuals' requests to exercise their rights pursuant to this section.

(2) An individual has the right to confirm whether or not a controller has enrolled an image or a facial template of that individual in a facial recognition service used in a physical premises open to the public.

(3) An individual has the right to correct or challenge a decision to enroll an image or a facial template of the individual in a facial recognition service used for a security or safety purpose in a physical premises open to the public.

(4) An individual has the right to delete an image or a facial template of the individual that has been enrolled in a facial recognition service used in a physical premises open to the public, except in the case of an image used for a security and safety purpose, provided that the controller has met each of the requirements pursuant to section 73-505(6), Idaho Code.

(5) An individual has the right to withdraw consent to enroll an image or a facial template of that individual in a facial recognition service used in a physical premises open to the public.

(6) A controller shall inform an individual of any action taken on a request pursuant to subsections (2) through (5) of this section without undue delay and in any event within thirty (30) days of receipt of the request. Such period may be extended by sixty (60) additional days where reasonably necessary, taking into account the complexity and number of the requests. The controller shall inform the individual of any such extension within thirty (30) days of receipt of the request, together with the reasons for the delay.

(a) If a controller does not take action on the request of an individual, the controller must inform the individual without undue delay and at the latest within thirty (30) days of receipt of the request of the reasons for not taking action.

(b) Information provided under this section must be provided by the controller free of charge to the individual. Where requests from an individual are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(i) Charge a reasonable fee to cover the administrative costs of complying with the request; or

(ii) Refuse to act on the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request.

(c) A controller is not required to comply with a request to exercise any of the rights pursuant to subsections (2) through (5) of this section if the controller is unable to determine, using commercially reasonable efforts, that the request is being made by the individual who is entitled to exercise such rights. In such cases, the controller may request the provision of additional information reasonably necessary to determine that the request is being made by the individual who is entitled to exercise such rights.

73-507. LIMITATIONS. The obligations imposed on controllers or processors under this chapter do not restrict a controller's or processor's ability to:

(1) Comply with federal, state, or local laws, rules, or regulations;

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities; and

(3) Investigate, establish, exercise, prepare for, or defend legal claims.

73-508. LIABILITY. (1) A violation of this chapter shall not serve as the basis for, or be subject to, a private right of action under this chapter or under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other laws, the constitution of the state of Idaho, or the constitution of the United States.

(2) Where more than one (1) controller or processor, or both a controller and a processor, contribute to the same violation of this chapter, the liability for such violation shall be allocated among the parties according to principles of comparative fault.

73-509. ENFORCEMENT. (1) The attorney general has exclusive authority to enforce the provisions of this chapter by bringing an action in the name of the state or as parens patriae on behalf of persons residing in the state.

(2) Any controller or processor that violates this chapter is subject to an injunction and liable for a civil penalty of no more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation.

73-510. ACCOUNTABILITY REPORT BY AGENCIES. (1) An agency using or intending to develop, procure, or use a facial recognition service must produce an accountability report for that system. The report must be clearly communicated to the public at least ninety (90) days prior to the agency putting the service into operational use and be posted on the public website of the agency.

(2) Each accountability report must include, at a minimum, clear and understandable statements of the following:

(a) The name of the facial recognition service, vendor, and version; and a description of its general capabilities and limitations, including reasonably foreseeable capabilities outside the scope of the proposed use of the agency;

(b) The type or types of data inputs that the facial recognition service uses when it is deployed; how that data is generated, collected, and processed; and the type or types of data the system is reasonably likely to generate;

(c) A description of the purpose and proposed use of the facial recognition service, including what decision or decisions it will be used to make or support; whether it is a final or support decision system; and its intended benefits, including any data or research demonstrating those benefits;

(d) A clear use and data management policy, including protocols for the following:

(i) How and when the facial recognition service will be deployed or used and by whom, including but not limited to the factors that will be used to determine where, when, and how the service is deployed, and other relevant information, such as whether the service will be operated continuously or used only under specific circumstances. If the facial recognition service will be operated or used by another entity on the agency's behalf, the accountability report must explicitly include a description of the other entity's access and any applicable protocols;

(ii) Any measures taken to minimize inadvertent collection of additional data beyond the amount necessary for the specific purpose or purposes for which the facial recognition service will be used;

(iii) Data integrity and retention policies applicable to the data collected using the facial recognition service, including how the agency will maintain and update records used in connection with the service, how long the agency will keep the data, and the processes by which data will be deleted;

(iv) Any additional rules that will govern use of the facial recognition service and what processes will be required prior to each use of the facial recognition service;

(v) Data security measures applicable to the facial recognition service, including how data collected using the facial recognition service will be securely stored and accessed, if and why an agency intends to share access to the facial recognition service or the data from that facial recognition service with any other entity, and the rules and procedures by which an agency sharing data with any other entity will ensure that such entities comply with the sharing agency's use and data management policy as part of the data-sharing agreement; and

(vi) The agency's training procedures, including those implemented in accordance with section 73-514, Idaho Code, and how the agency will ensure that all personnel who operate the facial recognition service or access its data are knowledgeable about and able to ensure compliance with the use and data management policy prior to use of the facial recognition service;

(e) The agency's testing procedures, including its processes for periodically undertaking operational tests of the facial recognition service in accordance with section 73-513, Idaho Code;

(f) A description of any potential impacts of the facial recognition service on civil rights and liberties, including potential impacts to privacy and potential disparate impacts on marginalized communities, and the specific steps the agency will take to mitigate the potential impacts and prevent unauthorized use of the facial recognition service; and

(g) The agency's procedures for receiving feedback, including the channels for receiving feedback from individuals affected by the use of the facial recognition service and from the community at large, as well as the procedures for responding to feedback.

(3) Prior to finalizing and implementing the accountability report, the agency must consider issues raised by the public through:

(a) A public review and comment period; and

(b) Community consultation meetings during the public review period.

(4) The accountability report must be updated every two (2) years, and each update must be subject to the public comment and community consultation processes described in this section.

(5) An agency seeking to use a facial recognition service for a purpose not disclosed in the agency's existing accountability report must first seek public comment and community consultation on the proposed new use and adopt an updated accountability report pursuant to the requirements contained in this section.

73-511. ANNUAL REPORTING ON THE ACCOUNTABILITY REPORT BY AGENCIES. (1) An agency using a facial recognition service is required to prepare and publish an annual report that discloses:

(a) The extent of its use of such services;

(b) An assessment of compliance with the terms of its accountability report;

(c) Any known or reasonably suspected violations of its accountability report, including complaints alleging violations; and

(d) Any revisions to its accountability report recommended by the agency during the next update of the policy.

(2) The annual report shall be submitted to the attorney general.

(3) All agencies must hold community meetings to review and discuss their annual report within sixty (60) days of its public release.

73-512. MEANINGFUL HUMAN REVIEW BY AGENCIES. An agency using a facial recognition service to make decisions that produce legal effects concerning individuals or similarly significant effects concerning individuals must ensure that those decisions are subject to meaningful human review. Decisions that produce legal effects concerning individuals or similarly significant effects concerning individuals shall include but not be limited to denial of consequential services or support, such as financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, and access to basic necessities such as food and water.

73-513. OPERATIONAL TESTING BY AGENCIES. Prior to deploying a facial recognition service in the context in which it will be used, an agency must test the facial recognition service in operational conditions. An agency must take reasonable steps to ensure best-quality results in operational conditions by following all reasonable guidance provided by the developer of the facial recognition service and mitigate any materially unfair performance differences across subpopulations.

73-514. TRAINING OF PERSONNEL BY AGENCIES. An agency using a facial recognition service must conduct periodic training of all individuals who operate a facial recognition service or who process personal data obtained from the use of a facial recognition service. Such training shall include but not be limited to coverage of:

(1) The capabilities and limitations of the facial recognition service;

(2) Procedures to interpret and act on the output of the facial recognition service; and

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

73-515. ONGOING SURVEILLANCE BY AGENCIES. (1) An agency shall not use a facial recognition service to engage in ongoing surveillance, unless such use is in support of law enforcement activities, may provide evidence of a serious criminal offense, and either:

(a) A search warrant has been obtained to permit the use of the facial recognition service for ongoing surveillance; or

(b) The agency reasonably determines that ongoing surveillance is necessary to prevent or respond to an emergency involving imminent danger or risk of death or serious physical injury to a person, but only if written approval is obtained from the agency's director or the di-

rector's designee prior to using the service and a search warrant is subsequently obtained within forty-eight (48) hours after the ongoing surveillance begins.

(2) An agency must not apply a facial recognition service to any individual based on his religious, political, or social views or activities, participation in a particular noncriminal organization or lawful event, or actual or perceived race, ethnicity, citizenship, place of origin, age, disability, gender, gender identity, sexual orientation, or other characteristic protected by law. The prohibition in this subsection shall not prohibit an agency from applying a facial recognition service to an individual who happens to possess one (1) or more of these characteristics where an officer of that agency holds a reasonable suspicion that the individual has committed, is committing, or is about to commit a serious criminal offense.

(3) An agency shall not use a facial recognition service to create a record describing any individual's exercise of rights guaranteed by the first amendment of the constitution of the United States or by sections 4 and 9 of article 1 of the constitution of the state of Idaho, unless:

(a) Such use is specifically authorized by applicable law and is pertinent to and within the scope of an authorized law enforcement activity; and

(b) There is reasonable suspicion to believe the individual has committed, is committing, or is about to commit a serious criminal offense.

73-516. DUE PROCESS PROTECTIONS AND RECORD-KEEPING BY AGENCIES. (1) An agency must disclose its use of a facial recognition service on a criminal defendant to that defendant in a timely manner prior to trial.

(2) An agency using a facial recognition service shall maintain records of its use of the service that are sufficient to facilitate public reporting and auditing of compliance with the applicable accountability report.

(3) In January of each year, any judge who has issued a warrant for ongoing surveillance, or an extension thereof, as described in section 73-515, Idaho Code, that expired during the preceding year, or who has denied approval of such a warrant during that year, shall report to the supreme court of Idaho:

(a) The fact that a warrant or extension was applied for;

(b) The fact that the warrant or extension was granted as applied for, was modified, or was denied;

(c) The period of ongoing surveillance authorized by the warrant and the number and duration of any extensions of the warrant;

(d) The identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and

(e) The nature of the public spaces where the surveillance was conducted.

73-517. PREEMPTION. This chapter supersedes and preempts laws, ordinances, regulations, or the equivalent adopted by any local entity regarding the development, use, or deployment of facial recognition services.

SECTION 2. SEVERABILITY. The provisions of this act are hereby declared to be severable and if any provision of this act or the application of such

provision to any person or circumstance is declared invalid for any reason, such declaration shall not affect the validity of the remaining portions of this act.