2020 South Dakota Legislature

Senate Bill 185

Introduced by: ***Senator*** *Langer*

An Act to regulate the use of facial recognition technology.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF SOUTH DAKOTA:

Section 1. That a NEW SECTION be added:

34-54-1. Definitions.

Terms used in this chapter mean:

(1) "Accountability report," a report developed in accordance with § 34-54-14;

(2) "Agency," a state or local government agency;

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

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

(5) "Enroll," "enrolled," or "enrolling," the process by which a facial recognition service creates a facial template from one or more images of a person and adds the facial template to a gallery used by the facial recognition service for recognition or persistent tracking of persons. The 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," technology that analyzes facial features and is used for recognition or persistent tracking of persons in still or video images;

(7) "Facial template," the machine-interpretable pattern of facial features that are extracted from one or more images of a person by a facial recognition service;

(8) "Identified or identifiable natural person," 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," review or oversight by a person who is trained in accordance with § 34-54-7 and who has the authority to alter the decision under review;

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

(11) "Persistent tracking," the use of a facial recognition service by a controller or an agency to track the movements of a person on a persistent basis without using the facial recognition service for recognition of that person. The 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 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 purchase or payment data, such that the person who has been tracked is identified or identifiable;

(12) "Personal data," any information that is linked or reasonably linkable to an identified or identifiable person. The term does not include de-identified data or publicly available information. For these purposes, publicly available information is information that is lawfully made available from federal, state, or local government records;

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

(14) "Processor," a person that processes personal data on behalf of a controller. An agency is not a processor;

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

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

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

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

(17) "Serious criminal offense," any felony under subdivision 22-1-2(9).

Section 2. That a NEW SECTION be added:

34-54-2. Applicability--Entities--Limitations.

Sections 34-54-3 through 34-54-12 apply to legal entities that conduct business in the state or produce products or services that are targeted to residents of the state.

The obligations imposed on any controller or processor 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.

Section 3. That a NEW SECTION be added:

34-54-3. Processors that provide facial recognition services--Requirements.

A processor that provides facial recognition services shall make available an application programming interface or other technical capability, chosen by the processor, to enable a controller or third party to conduct legitimate, independent, and reasonable tests of those facial recognition services for accuracy and unfair performance differences across distinct subpopulations. The 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 persons portrayed in the testing dataset. If the results of that independent testing identify material 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, the processor shall develop and implement a plan to mitigate the identified performance differences. Nothing in this section prevents a processor from prohibiting the use of the processor's facial recognition service by a competitor for competitive purposes.

A processor that provides facial recognition services shall provide documentation that includes general information that explains the capabilities and limitations of the services in plain language and enables testing of the services in accordance with this section.

A processor that provides facial recognition services shall prohibit, in the contract by which the controller is permitted to use the facial recognition service, the use of facial recognition services by the controller to unlawfully discriminate under federal or state law against persons or groups of persons.

Section 4. That a NEW SECTION be added:

34-54-4. Notice--Requirements--Contents.

If a facial recognition service is deployed in a physical premise open to the public, a controller shall provide a conspicuous and contextually appropriate notice on the purpose or purposes for which the facial recognition service is deployed and information about where persons can obtain additional information about the facial recognition service, including a link to any applicable online notice, terms, or policy that provides information about where and how a person may exercise any rights that the person has with respect to the facial recognition service.

Section 5. That a NEW SECTION be added:

34-54-5. Consent--Exception.

A controller shall obtain consent from a person prior to enrolling an image or a facial template of that person in a facial recognition service used in a physical premise open to the public.

A controller may enroll an image or a facial template of a person in a facial recognition service for a security or safety purpose without first obtaining consent from that person provided that each of the following requirements is met:

(1) The controller shall hold a reasonable suspicion, based on a specific incident, that the person has engaged in criminal activity, which includes shoplifting, fraud, stalking, or domestic violence;

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

(3) The controller shall review any such database used by the controller's facial recognition service no less than bi-annually to remove facial templates of persons in respect of whom the controller no longer holds a reasonable suspicion that they have engaged in criminal activity or that are more than three years old; and

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

Section 6. That a NEW SECTION be added:

34-54-6. Testing--Requirements.

Prior to deploying a facial recognition service in the context in which it will be used, an agency or a controller shall test the facial recognition service in operational conditions. An agency or a controller shall take commercially reasonable steps to ensure the best quality results in operational conditions by following all reasonable guidance provided by the developer of the facial recognition service.

Section 7. That a NEW SECTION be added:

34-54-7. Training--Requirements.

Any agency or controller using a facial recognition service shall conduct periodic training of all persons that operate a facial recognition service or that process personal data obtained from the use of facial recognition services. The training shall include:

(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) The meaningful human review requirement for decisions that produce legal effects concerning individual persons or similarly significant effects concerning individual persons.

Section 8. That a NEW SECTION be added:

34-54-8. Disclosure--Prohibitions.

A controller may not knowingly disclose personal data obtained from a facial recognition service to a law enforcement agency except if the disclosure is:

(1) Pursuant to the consent of the person to whom the personal data relates;

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

(3) 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

(4) To the National Center for Missing and Exploited Children, in connection with a report submitted thereto under Section 2258A of title 18 of the United States Code.

Section 9. That a NEW SECTION be added:

34-54-9. Personal rights--Request to controller--Process.

A person may exercise the rights set forth in this section by submitting a request, at any time, to a controller specifying which rights the person wishes to exercise. Except as provided in this chapter, the controller shall 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 any person's requests to exercise the person's rights pursuant to this section. A person has a right to:

(1) Confirm whether or not a controller has enrolled an image or a facial template of that person in a facial recognition service used in a physical premise open to the public;

(2) Correct or challenge a decision to enroll an image or a facial template of the person in a facial recognition service used for a security or safety purpose in a physical premise open to the public;

(3) Delete an image or a facial template of the person that has been enrolled in a facial recognition service used in a physical premise open to the public, except in the case of an image used for a security and safety purpose and provided that the controller has met each of the requirements of the security and safety exception under § 34-54-5; and

(4) Withdraw consent to enroll an image or a facial template of that person in a facial recognition service used in a physical premise open to the public.

A controller shall inform a person of any action taken on a request under this section without undue delay and in any event within thirty days of receipt of the request. That period may be extended by sixty additional days if reasonably necessary, taking into account the complexity and number of requests. The controller shall inform the person of any extension within thirty days of receipt of the request, together with the reasons for the delay.

If a controller does not take action on the request of a person, the controller shall inform the person without undue delay and at the latest within thirty days of receipt of the request of the reasons for not taking action.

Information provided under this section shall be provided by the controller free of charge to the person. If requests from a person 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.

A controller is not required to comply with a request to exercise any of the rights under this section if the controller is unable to determine, using commercially reasonable efforts, that the request is being made by the person who is entitled to exercise such rights. In any such case, the controller may request the provision of additional information reasonably necessary to determine that the request is being made by the person who is entitled to exercise such rights.

Section 10. That a NEW SECTION be added:

34-54-12. Enforcement.

The attorney general has exclusive authority to enforce this chapter by bringing an action in the name of the state, or as parens patriae on behalf of any person residing in the state, to enforce this chapter.

A violation of this chapter may not serve as the basis for, or be subject to, a private right of action under this chapter or under any other law. This may not be construed to relieve any party from any duties or obligations imposed under other laws, the state Constitution, or the United States Constitution.

Any controller or processor that violates this chapter is subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars for each violation or seven thousand five hundred dollars for each intentional violation.

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

Section 11. That a NEW SECTION be added:

34-54-13. Meaningful human review.

An agency or controller using a facial recognition service to make decisions that produce legal effects concerning persons or similarly significant effects concerning persons shall ensure that those decisions are subject to meaningful human review. Any decision that produces legal effects concerning a person or similarly significant effects concerning

a person shall include 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.

Section 12. That a NEW SECTION be added:

34-54-14. Accountability report.

An agency using or intending to develop, procure, or use a facial recognition service shall produce an accountability report for that system. The report shall be clearly communicated to the public at least ninety days prior to the agency putting the service into operational use, posted on the public website of the agency, and submitted to the Bureau of Information and Telecommunications. The bureau shall post each submitted accountability report on its public web site. Each accountability report shall include clear and understandable statements of the following:

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

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

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

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

(a) How and when the facial recognition service will be deployed or used and by whom including 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 shall explicitly include a description of the other entity's access and any applicable protocols;

(b) 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;

(c) 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;

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

(e) Any 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

(f) The agency's training procedures, including those implemented in accordance with § 34-54-7 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;

(5) The agency's testing procedures, including its processes for periodically undertaking operational tests of the facial recognition service in accordance with § 34-54-6;

(6) 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

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

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

Section 13. That a NEW SECTION be added:

34-54-15. Public review and comment.

Prior to finalizing and implementing the accountability report, the agency shall consider issues raised by the public through a public review and comment period and community consultation meetings during the public review period.

An agency seeking to use a facial recognition service for a purpose not disclosed in the agency's existing accountability report shall 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.

Section 14. That a NEW SECTION be added:

34-54-16. Annual report--Disclosures.

An agency using a facial recognition service is required to prepare and publish an annual report that discloses:

(1) The extent of their use of the service;

(2) An assessment of compliance with the terms of the agency's accountability report;

(3) Any known or reasonably suspected violation of the agency's accountability report, including any complaint alleging a violation; and

(4) Any revisions to the agency's accountability report recommended by the agency during the next update of the policy.

The annual report shall be submitted to the Bureau of Information and Telecommunications.

Each agency shall hold community meetings to review and discuss the agency's annual report within sixty days of the report's public release.

Section 15. That a NEW SECTION be added:

34-54-17. Ongoing surveillance--Prohibition--Exceptions.

An agency may not use a facial recognition service to engage in ongoing surveillance, unless the use is in support of law enforcement activities, may provide evidence of a serious criminal offense, and either:

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

(2) If 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 prior to using the service and a search warrant is subsequently obtained within forty-eight hours after the ongoing surveillance begins.

Section 16. That a NEW SECTION be added:

34-54-18. Application of service--Prohibitions.

An agency may not apply a facial recognition service to any person based on the person's 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 section or § 34-15-17 does not prohibit an agency from applying a facial recognition service to a person who happens to possess one or more of these characteristics if an officer of that agency holds a reasonable suspicion that that person has committed, is committing, or is about to commit a serious criminal offense.

Section 17. That a NEW SECTION be added:

34-54-19. Judges--Ongoing surveillance.

In January of each year, any judge who has issued a warrant for ongoing surveillance, or an extension thereof, under § 34-15-17 that expired during the preceding year, or who has denied approval of such a warrant during that year shall report to the Supreme Court:

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

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

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

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

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

Section 18. That a NEW SECTION be added:

34-54-20. Disclosure--Criminal defendant.

An agency shall disclose the agency's use of a facial recognition service on a criminal defendant to that defendant in a timely manner prior to trial.

Section 19. That a NEW SECTION be added:

34-54-21. Preemption.

This chapter supersedes and preempts laws, ordinances, regulations, or the equivalent adopted by any political subdivision of the state regarding the development, use, or deployment of facial recognition services.