2022 SESSION

INTRODUCED

INTRODUCED

SB741

1/21/22 15:42

22104919D

SENATE BILL NO. 741

Offered January 21, 2022

A BILL to amend and reenact §§ 15.2-1723.2 and 23.1-815.1 of the Code of Virginia, relating to facial recognition technology; authorized uses.

Patron—Surovell

Referred to Committee on the Judiciary

Be it enacted by the General Assembly of Virginia:

1. That §§ 15.2-1723.2 and 23.1-815.1 of the Code of Virginia are amended and reenacted as follows:

§ 15.2-1723.2. Facial recognition technology; approval.

A. For purposes of this section, "facial recognition technology" means an electronic system *or service* for ~~enrolling, capturing, extracting, comparing, and matching an individual's geometric facial data to identify individuals in photos, videos, or real time~~ *conducting an algorithmic comparison of images of a person's facial features for the purpose of verification or identification*. "Facial recognition technology" does not include the use of an automated or semi-automated process to redact a recording in order to protect the privacy of a subject depicted in the recording prior to release or disclosure of the recording outside of the law-enforcement agency if the process does not generate or result in the retention of any biometric data or surveillance information.

B. ~~No~~ *A* local law-enforcement agency ~~shall purchase or deploy~~ *may use* facial recognition technology ~~unless such purchase or deployment of facial recognition technology is expressly authorized by statute~~ *as described in this section only for investigating a specific criminal incident, or a specific citizen welfare situation*. ~~For purposes of this section, a statute that does not refer to facial recognition technology shall not be construed to provide express authorization. Such statute shall require that any facial recognition technology purchased or deployed by the local law-enforcement agency be maintained under the exclusive control of such local law-enforcement agency and that any data contained by such facial recognition technology be kept confidential, not be disseminated or resold, and be accessible only by a search warrant issued pursuant to Chapter 5 (§ 19.2-52 et seq.) of Title 19.2 or an administrative or inspection warrant issued pursuant to law.~~

C. *Pursuant to § 2.2-1112, the Division of Purchases and Supply (the Division) shall determine the appropriate facial recognition technology for use in accordance with this section. The Division shall not approve any facial recognition technology unless it has been evaluated by the National Institute of Standards and Technology (NIST) and determined to have an accuracy score of at least 98 percent true positives within all demographic groups. Such accuracy score shall be based on the most recent available Facial Recognition Vendor Test utilized by NIST. To ensure compliance with this section, the Division shall require all approved vendors to provide annually independent assessments and benchmarks offered by NIST. Any facial recognition technology utilized shall employ algorithms that have demonstrated the highest level of accuracy with minimal performance variations associated with race, skin tone, ethnicity, and gender.*

D. A match made through facial recognition technology shall not constitute probable cause for an arrest. A match made through facial recognition technology shall be admissible as exculpatory evidence.

E. A local law-enforcement agency may use facial recognition technology to compare or query against any lawfully acquired or accessed image or image database.

F. The Department of State Police shall develop, in consultation with stakeholder organizations, a model policy regarding the investigative uses of facial recognition technology. Such model policy shall be posted publicly no later than January 1, 2023, and shall include:

1. The nature and frequency of specialized training required for an individual to be authorized by a law-enforcement agency to utilize facial recognition as authorized by this section;

2. The extent to which a law-enforcement agency shall document (i) instances when facial recognition technology is used for both criminal and administrative investigations and (ii) how long such information is retained;

3. Procedures for the confirmation of any initial findings generated by facial recognition technology by a secondary examiner; and

4. Promulgation of standing orders, policies, or public materials by law-enforcement agencies that use facial recognition technology.

A local law-enforcement agency that uses facial recognition technology may adopt such model policy as developed by the Department of State Police in accordance with this subsection. If a local *law-enforcement agency uses facial recognition technology but does not adopt such model policy, such agency shall develop its own policy that meets or exceeds the standards set forth in such model policy. Any policy adopted or developed pursuant to this subsection shall be updated annually.*

G. Any local law-enforcement agency that uses facial recognition technology shall maintain records sufficient to facilitate discovery in criminal proceedings, post-conviction proceedings, public reporting, and auditing of compliance with such agency's facial recognition technology policies. Such agency that uses facial recognition technology shall collect data pertaining to (i) a complete history of each user's queries; (ii) the total number of queries conducted; (iii) the number of queries that resulted in a list of possible candidates; (iv) how many times an examiner offered law enforcement an investigative lead based on his findings; (v) how many cases were closed due to an investigative lead from facial recognition technology; (vi) what types of criminal offenses are being investigated; (vii) the nature of the image repository being compared or queried; and (viii) if applicable, any other entities with whom the agency shared facial recognition data.

H. Any chief of police whose agency uses facial recognition technology shall be responsible for publishing in print or on a public website an annual report by April 1 each year to provide information to the public regarding the agency's use of facial recognition technology. The report shall include all data required by subsection G. If any information or data (i) contains an articulable concern for any person's safety; (ii) is otherwise prohibited for public disclosure by federal or state statute; or (iii) if disclosed, may compromise sensitive criminal justice information, such information or data may be excluded from public disclosure. The annual report shall include (a) any instances of unauthorized access of the facial recognition technology, including any unauthorized access by employees of a local law-enforcement agency; (b) vendor information, including the specific algorithms employed; and (c) if applicable, data or links related to third-party testing of such algorithms, including any reference to variations in demographic performance.

I. A local law-enforcement agency shall notify in writing the governing body of the locality that such agency serves no less than 30 days before such agency procures facial recognition technology. The provisions of this subsection shall be deemed satisfied if the governing body of a locality directs the law-enforcement agency serving under the authority of the locality to procure facial recognition technology.

J. Nothing in this section shall apply to commercial air service airports.

§ 23.1-815.1. Facial recognition technology; approval.

A. For purposes of this ~~subsection~~ *section*, "facial recognition technology" means an electronic system *or service* for ~~enrolling, capturing, extracting, comparing, and matching an individual's geometric facial data to identify individuals in photos, videos, or real time~~ *conducting an algorithmic comparison of images of a person's facial features for the purpose of verification or identification*. "Facial recognition technology" does not include the use of an automated or semi-automated process to redact a recording in order to protect the privacy of a subject depicted in the recording prior to release or disclosure of the recording outside of the law-enforcement agency if the process does not generate or result in the retention of any biometric data or surveillance information.

B. ~~No~~ *A* campus police department ~~shall purchase or deploy~~ *may use* facial recognition technology ~~unless such purchase or deployment of facial recognition technology is expressly authorized by statute~~*as described in this section only for investigating a specific criminal incident or a specific citizen welfare situation*. ~~For purposes of this section, a statute that does not refer to facial recognition technology shall not be construed to provide express authorization. Such statute shall require that any facial recognition technology purchased or deployed by the campus police department be maintained under the exclusive control of such campus police department and that any data contained by such facial recognition technology be kept confidential, not be disseminated or resold, and be accessible only by a search warrant issued pursuant to Chapter 5 (§ 19.2-52 et seq.) of Title 19.2 or an administrative or inspection warrant issued pursuant to law.~~

C. Pursuant to § 2.2-1112, the Division of Purchases and Supply (the Division) shall determine the appropriate facial recognition technology for use in accordance with this section. The Division shall not approve any facial recognition technology unless it has been evaluated by the National Institute of Standards and Technology (NIST) and determined to have an accuracy score of at least 98 percent true positives within all demographic groups. Such accuracy score shall be based on the most recent available Facial Recognition Vendor Test utilized by NIST. To ensure compliance with this section, the Division shall require all approved vendors to provide annually independent assessments and benchmarks offered by NIST. Any facial recognition technology utilized shall employ algorithms that have demonstrated the highest level of accuracy with minimal performance variations associated with race, skin tone, ethnicity, and gender.

D. A match made through facial recognition technology shall not constitute probable cause for an arrest. A match made through facial recognition technology shall be admissible as exculpatory evidence.

E. A campus police department may use facial recognition technology to compare or query against *any lawfully acquired or accessed image or image database.*

F. A campus police department shall publicly post its policy on use of facial recognition technology before employing such facial recognition technology to investigate a specific criminal incident or citizen welfare situation. Pursuant to subsection F of § 15.2-1723.2, a campus police department may either (i) adopt the model policy developed by the Department of State Police or (ii) develop its own policy that meets or exceeds the standards set forth in such model policy. Any policy adopted or developed pursuant to this subsection shall be updated annually.

G. Any campus police department that uses facial recognition technology shall maintain records sufficient to facilitate discovery in criminal proceedings, post-conviction proceedings, public reporting, and auditing of compliance with such department's facial recognition technology policies. Such department that uses facial recognition technology shall collect data pertaining to (i) a complete history of each user's queries; (ii) the total number of queries conducted; (iii) the number of queries that resulted in a list of possible candidates; (iv) how many times an examiner offered campus police an investigative lead based on his findings; (v) how many cases were closed due to an investigative lead from facial recognition technology; (vi) what types of criminal offenses are being investigated; (vii) the nature of the image repository being compared or queried; and (viii) if applicable, any other entities with whom the department shared facial recognition data.

H. Any chief of a campus police department whose agency uses facial recognition technology shall be responsible for publishing in print or on a public website an annual report by April 1 each year to provide information to the public regarding the department's use of facial recognition technology. The report shall include all data required by subsection G of § 15.2-1723.2. If any information or data (i) contains an articulable concern for any person's safety; (ii) is otherwise prohibited for public disclosure by federal or state statute; or (iii) if disclosed, may compromise sensitive criminal justice information, such information or data may be excluded from public disclosure. The annual report shall include (a) any instances of unauthorized access of the facial recognition technology, including any unauthorized access by employees of a campus police department; (b) vendor information, including the specific algorithms employed; and (c) if applicable, data or links related to third-party testing of such algorithms, including any reference to variations in demographic performance.

I. A campus police department shall notify in writing the public institution of higher education that such department serves no less than 30 days before such department procures facial recognition technology. The provisions of this subsection shall be deemed satisfied if the public institution of higher education directs the campus police department to procure facial recognition technology.

INTRODUCED

SB741