SENATE BILL NO. 741

AMENDMENT IN THE NATURE OF A SUBSTITUTE

(Proposed by the Senate Committee on General Laws and Technology

on ________________)

(Patron Prior to Substitute--Senator Surovell)

A BILL to amend and reenact §§ 15.2-1723.2 and 23.1-815.1 of the Code of Virginia and to amend the Code of Virginia by adding a section number 52-4.5, relating to facial recognition technology; Department of State Police and authorized uses.

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 and that the Code of Virginia is amended by adding a section numbered 52-4.5 as follows:

§ 15.2-1723.2. Facial recognition technology; approval.

A. For purposes of this section~~, "facial recognition technology"~~:

"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 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.

"Publicly post" means to post on a website that is maintained by the entity or on any other website on which the entity generally posts information and that is available to the public or that clearly describes how the public may access such data.

"State Police Model Facial Recognition Technology Policy" means the model policy developed and published by the Department of State Police pursuant to § 52-4.5.

B. ~~No~~ 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) as part of the Face Recognition Vendor Test. Any facial recognition technology utilized shall utilize algorithms that have demonstrated (i) an accuracy score of at least 98 percent true positives within one or more datasets relevant to the application in a NIST Facial Recognition Vendor Test report and (ii) with minimal performance variations across demographics associated with race, skin tone, ethnicity, or gender. The Division shall require all approved vendors to annually provide independent assessments and benchmarks offered by NIST to confirm continued compliance with this section.

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

~~C.~~ D. A local law-enforcement agency shall publicly post and annually update its policy regarding the use of facial recognition technology before employing such facial recognition technology to investigate a specific criminal incident or citizen welfare situation. A local law-enforcement agency that uses facial recognition technology may adopt the State Police Model Facial Recognition Technology Policy. If a local law-enforcement agency uses facial recognition technology but does not adopt such model policy, such agency shall develop its own policy within 90 days of publication of the State Police

Model Facial Recognition Technology Policy that meets or exceeds the standards set forth in such model policy.

E. 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 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.

F. Any chief of police whose agency uses facial recognition technology shall publicly post and annually update a 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 clauses (ii) through (viii) of subsection E in addition to (i) all instances of unauthorized access of the facial recognition technology, including any unauthorized access by employees of a local law-enforcement agency; (ii) vendor information, including the specific algorithms employed; and (iii) if applicable, data or links related to third-party testing of such algorithms, including any reference to variations in demographic performance. If any information or data (a) contains an articulable concern for any person's safety; (b) is otherwise prohibited from public disclosure by federal or state statute; or (c) if disclosed, may compromise sensitive criminal justice information, such information or data may be excluded from public disclosure. Nothing herein shall limit disclosure of data collected pursuant to subsection E when such disclosure is related to a writ of habeas corpus.

For purposes of this subsection, "sensitive criminal justice information" means information related to (1) a particular ongoing criminal investigation or proceeding, (2) the identity of a confidential source, or (3) law-enforcement investigative techniques and procedures.

F. At least 30 days prior to procuring facial recognition technology, a local law-enforcement agency shall notify in writing the governing body of the locality that such agency serves of such intended procurement, but such notice shall not be required if such procurement is directed by the governing body.

G. 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"~~:

"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 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.

"Publicly post" means to post on a website that is maintained by the entity or on any other website on which the entity generally posts information and that is available to the public or that clearly describes how the public may access such data.

"State Police Model Facial Recognition Technology Policy" means the model policy developed and published by the Department of State Police pursuant to § 52-4.5.

B. ~~No~~ 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) as part of the Face Recognition Vendor Test. Any facial recognition technology utilized shall utilize algorithms that have demonstrated (i) an accuracy score of at least 98 percent true positives within one or more datasets relevant to the application in a NIST Facial Recognition Vendor Test report, and (ii) with minimal performance variations across demographics associated with race, skin tone, ethnicity, or gender. The Division shall require all approved vendors to annually provide independent assessments and benchmarks offered by NIST to confirm continued compliance with this section.

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

D. 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. A campus police department that uses facial recognition technology may adopt the State Police Model Facial Recognition Technology Policy. If a campus police department uses facial recognition technology but does not adopt the State Police Model Facial Recognition Technology Policy, such department shall develop its own policy within 90 days of publication of the State Police Model Facial Recognition Technology 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.

E. 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.

F. Any chief of a campus police department whose agency uses facial recognition technology shall publicly post and annually update a 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 clauses (ii) through (viii) of subsection E in addition to (i) all instances of unauthorized access of the facial recognition technology, including any unauthorized access by employees the campus police department; (ii) vendor information, including the specific algorithms employed; and (iii) if applicable, data or links related to third-party testing of such algorithms, including any reference to variations in demographic performance. If any information or data (a) contains an articulable concern for any person's safety; (b) is otherwise prohibited from public disclosure by federal or state statute; or (c) if disclosed, may compromise sensitive criminal justice information, such information or data may be excluded from public disclosure. Nothing herein shall limit disclosure of data collected pursuant to subsection E when such disclosure is related to a writ of habeas corpus.

For purposes of this subsection, "sensitive criminal justice information" means information related to (1) a particular ongoing criminal investigation or proceeding, (2) the identity of a confidential source, or (3) law-enforcement investigative techniques and procedures.

G. At least 30 days prior to procuring facial recognition technology, a campus police department shall notify in writing the institution of higher education that such department serves of such intended procurement, but such notice shall not be required if such procurement is directed by the governing body.

§ 52-4.5. Department to establish a State Police Model Facial Recognition Technology Policy.

The Department shall create a model policy regarding the use of facial recognition technology, which shall be known as the State Police Model Facial Recognition Technology Policy. Such policy shall be publicly posted no later than January 1, 2023, be annually updated thereafter, and 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 authorized purposes 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.

For purposes of this section, "publicly posted" shall have the same meaning as defined in § 15.2-1723.2.

#