

22106194D

SENATE BILL NO. 741

AMENDMENT IN THE NATURE OF A SUBSTITUTE

(Proposed by the Senate Committee on General Laws and Technology
on February 9, 2022)

(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. 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 be included in an affidavit to establish probable cause for purposes of issuance of a search warrant or an arrest warrant but shall be admissible as exculpatory evidence.

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

60 collect data pertaining to (i) a complete history of each user's queries; (ii) the total number of queries
 61 conducted; (iii) the number of queries that resulted in a list of possible candidates; (iv) how many times
 62 an examiner offered law enforcement an investigative lead based on his findings; (v) how many cases
 63 were closed due to an investigative lead from facial recognition technology; (vi) what types of criminal
 64 offenses are being investigated; (vii) the nature of the image repository being compared or queried; and
 65 (viii) if applicable, any other entities with whom the agency shared facial recognition data.

66 F. Any chief of police whose agency uses facial recognition technology shall publicly post and
 67 annually update a report by April 1 each year to provide information to the public regarding the
 68 agency's use of facial recognition technology. The report shall include all data required by clauses (ii)
 69 through (viii) of subsection E in addition to (i) all instances of unauthorized access of the facial
 70 recognition technology, including any unauthorized access by employees of a local law-enforcement
 71 agency; (ii) vendor information, including the specific algorithms employed; and (iii) if applicable, data
 72 or links related to third-party testing of such algorithms, including any reference to variations in
 73 demographic performance. If any information or data (a) contains an articulable concern for any
 74 person's safety; (b) is otherwise prohibited from public disclosure by federal or state statute; or (c) if
 75 disclosed, may compromise sensitive criminal justice information, such information or data may be
 76 excluded from public disclosure. Nothing herein shall limit disclosure of data collected pursuant to
 77 subsection E when such disclosure is related to a writ of habeas corpus.

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

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

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

86 **§ 23.1-815.1. Facial recognition technology; approval.**

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

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

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

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

101 B. ~~No~~ Pursuant to § 2.2-1112, the Division of Purchases and Supply (the Division) shall determine
 102 the appropriate facial recognition technology for use in accordance with this section. The Division shall
 103 not approve any facial recognition technology unless it has been evaluated by the National Institute of
 104 Standards and Technology (NIST) as part of the Face Recognition Vendor Test. Any facial recognition
 105 technology utilized shall utilize algorithms that have demonstrated (i) an accuracy score of at least 98
 106 percent true positives within one or more datasets relevant to the application in a NIST Facial
 107 Recognition Vendor Test report, and (ii) with minimal performance variations across demographics
 108 associated with race, skin tone, ethnicity, or gender. The Division shall require all approved vendors to
 109 annually provide independent assessments and benchmarks offered by NIST to confirm continued
 110 compliance with this section.

111 C. A campus police department shall purchase or deploy may use facial recognition technology unless
 112 such purchase or deployment of facial recognition technology is expressly authorized by statute as
 113 described in this section only for investigating a specific criminal incident or a specific citizen welfare
 114 situation. For purposes of this section, a statute that does not refer to facial recognition technology shall
 115 not be construed to provide express authorization. Such statute shall require that any facial recognition
 116 technology purchased or deployed by the campus police department be maintained under the exclusive
 117 control of such campus police department and that any data contained by such facial recognition
 118 technology be kept confidential, not be disseminated or resold, and be accessible only by a search
 119 warrant issued pursuant to Chapter 5 (§ 19.2-52 et seq.) of Title 19.2 or an administrative or inspection
 120 warrant issued pursuant to law. A match made through facial recognition technology shall not be
 121 included in an affidavit to establish probable cause for purposes of issuance of a search warrant or an

122 arrest warrant but shall be admissible as exculpatory evidence.

123 D. A campus police department shall publicly post its policy on use of facial recognition technology
124 before employing such facial recognition technology to investigate a specific criminal incident or citizen
125 welfare situation. A campus police department that uses facial recognition technology may adopt the
126 State Police Model Facial Recognition Technology Policy. If a campus police department uses facial
127 recognition technology but does not adopt the State Police Model Facial Recognition Technology Policy,
128 such department shall develop its own policy within 90 days of publication of the State Police Model
129 Facial Recognition Technology Policy that meets or exceeds the standards set forth in such model
130 policy. Any policy adopted or developed pursuant to this subsection shall be updated annually.

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

141 F. Any chief of a campus police department whose agency uses facial recognition technology shall
142 publicly post and annually update a report by April 1 each year to provide information to the public
143 regarding the agency's use of facial recognition technology. The report shall include all data required
144 by clauses (ii) through (viii) of subsection E in addition to (i) all instances of unauthorized access of the
145 facial recognition technology, including any unauthorized access by employees the campus police
146 department; (ii) vendor information, including the specific algorithms employed; and (iii) if applicable,
147 data or links related to third-party testing of such algorithms, including any reference to variations in
148 demographic performance. If any information or data (a) contains an articulable concern for any
149 person's safety; (b) is otherwise prohibited from public disclosure by federal or state statute; or (c) if
150 disclosed, may compromise sensitive criminal justice information, such information or data may be
151 excluded from public disclosure. Nothing herein shall limit disclosure of data collected pursuant to
152 subsection E when such disclosure is related to a writ of habeas corpus.

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

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

160 **§ 52-4.5. Department to establish a State Police Model Facial Recognition Technology Policy.**

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

- 164 1. The nature and frequency of specialized training required for an individual to be authorized by a
- 165 law-enforcement agency to utilize facial recognition as authorized by this section;
- 166 2. The extent to which a law-enforcement agency shall document (i) instances when facial
- 167 recognition technology is used for authorized purposes and (ii) how long such information is retained;
- 168 3. Procedures for the confirmation of any initial findings generated by facial recognition technology
- 169 by a secondary examiner; and
- 170 4. Promulgation of standing orders, policies, or public materials by law-enforcement agencies that
- 171 use facial recognition technology.

172 For purposes of this section, "publicly posted" shall have the same meaning as defined in
173 § 15.2-1723.2.