

SENATE BILL NO. 741

AMENDMENT IN THE NATURE OF A SUBSTITUTE

(Proposed by the House Committee on Public Safety

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 numbered 52-4.5, relating to facial recognition technology; Department of State Police and authorized uses; report; penalty.

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; penalty.

A. For purposes of this section, ~~"facial;~~

"Authorized use" means the use of facial recognition technology to (i) help identify an individual when there is a reasonable suspicion the individual has committed a crime; (ii) help identify a crime victim, including a victim of online sexual abuse material; (iii) help identify a person who may be a missing person or witness to criminal activity; (iv) help identify a victim of human trafficking or an individual involved in the trafficking of humans, weapons, drugs, or wildlife; (v) help identify an online recruiter of criminal activity, including but not limited to human, weapon, drug, and wildlife trafficking; (vi) help a person who is suffering from a mental or physical disability impairing his ability to communicate and be understood; (vii) help identify a deceased person; (viii) help identify a person who is incapacitated or otherwise unable to identify himself; (ix) help identify a person who is reasonably believed to be a danger to himself or others; (x) help identify an individual lawfully detained; (xi) help mitigate an imminent threat to public safety, a significant threat to life, or a threat to national security, including acts of terrorism; (xii) ensure officer safety as part of the vetting of undercover law enforcement; (xiii) determine whether an individual may have unlawfully obtained one or more state driver's licenses, financial instruments, or other

27 official forms of identification using information that is fictitious or associated with a victim of identity
28 theft; or (xiv) help identify a person who an officer reasonably believes is concealing his true identity and
29 about whom the officer has a reasonable suspicion has committed a crime other than concealing his
30 identity.

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

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

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

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

53 C. A local law-enforcement agency shall purchase or deploy may use facial recognition technology
54 unless such purchase or deployment of facial recognition technology is expressly authorized by statute for
55 authorized uses. For purposes of this section, a statute that does not refer to facial recognition technology
56 shall not be construed to provide express authorization. Such statute shall require that any facial
57 recognition technology purchased or deployed by the local law enforcement agency be maintained under
58 the exclusive control of such local law enforcement agency and that any data contained by such facial
59 recognition technology be kept confidential, not be disseminated or resold, and be accessible only by a
60 search warrant issued pursuant to Chapter 5 (§ 19.2 52 et seq.) of Title 19.2 or an administrative or
61 inspection warrant issued pursuant to law. A match made through facial recognition technology shall not
62 be included in an affidavit to establish probable cause for purposes of issuance of a search warrant or an
63 arrest warrant but shall be admissible as exculpatory evidence.

64 C-D. A local law-enforcement agency shall publicly post and annually update its policy regarding
65 the use of facial recognition technology before employing such facial recognition technology to
66 investigate a specific criminal incident or citizen welfare situation. A local law-enforcement agency that
67 uses facial recognition technology may adopt the State Police Model Facial Recognition Technology
68 Policy. If a local law-enforcement agency uses facial recognition technology but does not adopt such
69 model policy, such agency shall develop its own policy within 90 days of publication of the State Police
70 Model Facial Recognition Technology Policy that meets or exceeds the standards set forth in such model
71 policy. A local law-enforcement agency shall not utilize any facial recognition technology until after the
72 publication of the State Police Model Facial Recognition Technology Policy and after publication of the
73 agency's policy regarding the use of facial recognition technology.

74 E. Any local law-enforcement agency that uses facial recognition technology shall maintain
75 records sufficient to facilitate discovery in criminal proceedings, post-conviction proceedings, public
76 reporting, and auditing of compliance with such agency's facial recognition technology policies. Such
77 agency shall collect data pertaining to (i) a complete history of each user's queries; (ii) the total number
78 of queries conducted; (iii) the number of queries that resulted in a list of possible candidates; (iv) how
79 many times an examiner offered law enforcement an investigative lead based on his findings; (v) how

80 many cases were closed due to an investigative lead from facial recognition technology; (vi) what types
81 of criminal offenses are being investigated; (vii) the nature of the image repository being compared or
82 queried; (viii) demographic information for the individuals whose images are queried; and (ix) if
83 applicable, any other entities with which the agency shared facial recognition data.

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

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

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

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

103 I. Any facial recognition technology operator employed by a local law-enforcement agency who
104 (i) violates the agency's policy for the use of facial recognition technology or (ii) conducts a search for
105 any reason other than an authorized use is guilty of a Class 3 misdemeanor and shall be required to
106 complete training on the agency's policy on and authorized uses of facial recognition technology before

107 being reinstated to operate such facial recognition technology. The local law-enforcement agency shall
108 terminate from employment any facial recognition technology operator who violates clause (i) or (ii) for
109 a second time.

110 **§ 23.1-815.1. Facial recognition technology; approval; penalty.**

111 A. For purposes of this subsection, "facial section:"

112 "Authorized use" means the use of facial recognition technology to (i) help identify an individual
113 when there is a reasonable suspicion the individual has committed a crime; (ii) help identify a crime victim,
114 including a victim of online sexual abuse material; (iii) help identify a person who may be a missing
115 person or witness to criminal activity; (iv) help identify a victim of human trafficking or an individual
116 involved in the trafficking of humans, weapons, drugs, or wildlife; (v) help identify an online recruiter of
117 criminal activity, including but not limited to human, weapon, drug, and wildlife trafficking; (vi) help a
118 person who is suffering from a mental or physical disability impairing his ability to communicate and be
119 understood; (vii) help identify a deceased person; (viii) help identify a person who is incapacitated or
120 otherwise unable to identify himself; (ix) help identify a person who is reasonably believed to be a danger
121 to himself or others; (x) help identify an individual lawfully detained; (xi) help mitigate an imminent threat
122 to public safety, a significant threat to life, or a threat to national security, including acts of terrorism; (xii)
123 ensure officer safety as part of the vetting of undercover law enforcement; (xiii) determine whether an
124 individual may have unlawfully obtained one or more state driver's licenses, financial instruments, or other
125 official forms of identification using information that is fictitious or associated with a victim of identity
126 theft; or (xiv) help identify a person who an officer reasonably believes is concealing his true identity and
127 about whom the officer has a reasonable suspicion has committed a crime other than concealing his
128 identity.

129 "Facial recognition technology" means an electronic system or service for enrolling, capturing,
130 extracting, comparing, and matching an individual's geometric facial data to identify individuals in photos,
131 videos, or real time conducting an algorithmic comparison of images of a person's facial features for the
132 purpose of identification. "Facial recognition technology" does not include the use of an automated or
133 semi-automated process to redact a recording in order to protect the privacy of a subject depicted in the

134 recording prior to release or disclosure of the recording outside of the law-enforcement agency if the
135 process does not generate or result in the retention of any biometric data or surveillance information.

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

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

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

151 C. A campus police department shall purchase or deploy may use facial recognition technology
152 unless such purchase or deployment of facial recognition technology is expressly authorized by statute for
153 authorized uses. For purposes of this section, a statute that does not refer to facial recognition technology
154 shall not be construed to provide express authorization. Such statute shall require that any facial
155 recognition technology purchased or deployed by the campus police department be maintained under the
156 exclusive control of such campus police department and that any data contained by such facial recognition
157 technology be kept confidential, not be disseminated or resold, and be accessible only by a search warrant
158 issued pursuant to Chapter 5 (§ 19.2-52 et seq.) of Title 19.2 or an administrative or inspection warrant
159 issued pursuant to law. A match made through facial recognition technology shall not be included in an

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

162 D. A campus police department shall publicly post its policy on use of facial recognition
163 technology before employing such facial recognition technology to investigate a specific criminal incident
164 or citizen welfare situation. A campus police department that uses facial recognition technology may adopt
165 the State Police Model Facial Recognition Technology Policy. If a campus police department uses facial
166 recognition technology but does not adopt the State Police Model Facial Recognition Technology Policy,
167 such department shall develop its own policy within 90 days of publication of the State Police Model
168 Facial Recognition Technology Policy that meets or exceeds the standards set forth in such model policy.
169 Any policy adopted or developed pursuant to this subsection shall be updated annually. A campus police
170 department shall not utilize any facial recognition technology until the publication of the State Police
171 Model Facial Recognition Technology Policy and publication of the department's policy regarding use of
172 facial recognition technology.

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

184 F. Any chief of a campus police department whose agency uses facial recognition technology shall
185 publicly post and annually update a report by April 1 each year to provide information to the public
186 regarding the agency's use of facial recognition technology. The report shall include all data required by

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

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

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

202 H. Any facial recognition technology operator employed by a campus police department who (i)
203 violates the department's policy for the use of facial recognition technology or (ii) conducts a search for
204 any reason other than an authorized use is guilty of a Class 3 misdemeanor and shall be required to
205 complete training on the department's policy on and authorized uses of facial recognition technology
206 before being reinstated to operate such facial recognition technology. The campus police department shall
207 terminate from employment any facial recognition technology operator who violates clause (i) or (ii) for
208 a second time.

209 **§ 52-4.5. Department to establish a State Police Model Facial Recognition Technology Policy.**

210 The Department shall create a model policy regarding the use of facial recognition technology,
211 which shall be known as the State Police Model Facial Recognition Technology Policy. The Department
212 shall publicly post such policy no later than January 1, 2023, and such policy shall be updated annually
213 thereafter and shall include:

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

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

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

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

222 For purposes of this section, "publicly post" shall have the same meaning as defined in § 15.2-
223 1723.2.

224 **2. That the Department of Criminal Justice Services (the Department) shall analyze and report on**
225 **the usage data of facial recognition technology reported and published by local law-enforcement**
226 **agencies and campus police departments pursuant to the provisions of this act. The Department**
227 **shall include in its report an analysis of and recommendations for (i) improving the use of facial**
228 **recognition technology as it relates to demographics associated with race, skin tone, ethnicity, and**
229 **gender; (ii) specialized training, data storage, data retention, and the use of a second examiner**
230 **pursuant to the State Police Model Facial Recognition Technology Policy established by § 52-4.5 of**
231 **the Code of Virginia, as created by this act; and (iii) investigations and investigative outcomes**
232 **related to the accuracy of identification across different demographic groups. The Department shall**
233 **submit its report to the Chairmen of the Senate Committee on the Judiciary and the House**
234 **Committee on Public Safety by November 1, 2025.**

235 **3. That the provisions of this act shall expire on July 1, 2026.**

236 #