22106444D

1  **HOUSE BILL NO. 1339**
2  AMENDMENT IN THE NATURE OF A SUBSTITUTE
3  (Proposed by the House Committee on Public Safety)
4  (Patron Prior to Substitute—Delegate Leftwich)
5  House Amendments in [ ] — February 14, 2022
6  *A BILL to amend and reenact §§ 15.2-1723.2 and 23.1-815.1 of the Code of Virginia and to amend the*
7  *Code of Virginia by adding a section numbered 52-4.5, relating to facial recognition technology;*
8  *Department of State Police and authorized uses* [ *; report; penalty* ] *.*
9  **Be it enacted by the General Assembly of Virginia:**
10  **1. That §§ 15.2-1723.2 and 23.1-815.1 of the Code of Virginia are amended and reenacted and that**
11  **the Code of Virginia is amended by adding a section numbered 52-4.5 as follows:**
12  **§ 15.2-1723.2. Facial recognition technology; approval** [ **; penalty** ] **.**
13  A. For purposes of this section, "facial*:*
14  *"Authorized use" means the use of facial recognition technology to (i) help identify an individual*
15  *when there is a reasonable suspicion the individual has committed* [ *, is committing, or is planning the*
16  *commission of* ] *a crime; (ii) help identify a crime victim, including a victim of online sexual abuse*
17  *material; (iii) help identify a person who may be a missing person or witness to criminal activity; (iv)*
18  *help identify a victim of human trafficking or an individual involved in the trafficking of humans,*
19  *weapons, drugs, or wildlife; (v) help identify an online recruiter of criminal activity, including but not*
20  *limited to human, weapon, drug, and wildlife trafficking; (vi) help a person who is suffering from a*
21  *mental or physical disability impairing his ability to communicate and be understood; (vii) help identify*
22  *a deceased person; (viii) help identify a person who is incapacitated or otherwise unable to identify*
23  *himself; (ix) help identify a person who is reasonably believed to be a danger to himself or others; (x)*
24  *help identify an individual lawfully detained; (xi) help mitigate an imminent threat to public safety, a*
25  *significant threat to life, or a threat to national security, including acts of terrorism; (xii) ensure officer*
26  *safety as part of the vetting of undercover law enforcement; (xiii) determine whether an individual may*
27  *have unlawfully obtained one or more state driver's licenses, financial instruments, or other official*
28  *forms of identification using information that is fictitious or associated with a victim of identity theft; or*
29  *(xiv) help identify a person who an officer reasonably believes is concealing his true identity and about*
30  *whom the officer has a reasonable suspicion has committed a crime other than concealing his 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~~
33  ~~photos, videos, or real~~ time *conducting an algorithmic comparison of images of a person's facial*
34  *features for the purpose of identification.* "Facial recognition technology" does not include the use of an
35  automated or semi-automated process to redact a recording in order to protect the privacy of a subject
36  depicted in the recording prior to release or disclosure of the recording outside of the law-enforcement
37  agency if the process does not generate or result in the retention of any biometric data or surveillance
38  information.
39  *"Publicly post" means to post on a website that is maintained by the entity or on any other website*
40  *on which the entity generally posts information and that is available to the public or that clearly*
41  *describes how the public may access such data.*
42  *"State Police Model Facial Recognition Technology Policy" means the model policy developed and*
43  *published by the Department of State Police pursuant to § 52-4.5.*
44  B. ~~No~~ *Pursuant to § 2.2-1112, the Division of Purchases and Supply (the Division) shall determine*
45  *the appropriate facial recognition technology for use in accordance with this section. The Division shall*
46  *not approve any facial recognition technology unless it has been evaluated by the National Institute of*
47  *Standards and Technology (NIST) as part of the Face Recognition Vendor Test. Any facial recognition*
48  *technology utilized shall utilize algorithms that have demonstrated (i) an accuracy score of at least 98*
49  *percent true positives within one or more datasets relevant to the application in a NIST Facial*
50  *Recognition Vendor Test report and (ii) minimal performance variations across demographics associated*
51  *with race, skin tone, ethnicity, or gender. The Division shall require all approved vendors to annually*
52  *provide independent assessments and benchmarks offered by NIST to confirm continued compliance with*
53  *this section.*
54  *C. A* local law-enforcement agency ~~shall purchase or deploy~~ *may use* facial recognition technology
55  ~~unless such purchase or deployment of facial recognition technology is expressly authorized by statute~~
56  *for authorized uses.* ~~For purposes of this section, a statute that does not refer to facial recognition~~
57  ~~technology shall not be construed to provide express authorization. Such statute shall require that any~~
58  ~~facial recognition technology purchased or deployed by the local law-enforcement agency be maintained~~
59  ~~under the exclusive control of such local law-enforcement agency and that any data contained by such~~

60  facial recognition technology be kept confidential, not be disseminated or resold, and be accessible only
61  by a search warrant issued pursuant to Chapter 5 (§ 19.2-52 et seq.) of Title 19.2 or an administrative or
62  inspection warrant issued pursuant to law. *A match made through facial recognition technology shall not*
63  *constitute probable cause for an arrest 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*
71  *model policy.*
72      *E. Any local law-enforcement agency that uses facial recognition technology shall maintain records*
73  *sufficient to facilitate discovery in criminal proceedings, post-conviction proceedings, public reporting,*
74  *and auditing of compliance with such agency's facial recognition technology policies. Such agency shall*
75  *collect data pertaining to (i) a complete history of each user's queries; (ii) the total number of queries*
76  *conducted; (iii) the number of queries that resulted in a list of possible candidates; (iv) how many times*
77  *an examiner offered law enforcement an investigative lead based on his findings; (v) how many cases*
78  *were closed due to an investigative lead from facial recognition technology; (vi) what types of criminal*
79  *offenses are being investigated; (vii) the nature of the image repository being compared or queried;* [
80  *and* ] *(viii)* [ *demographic information for the individuals whose images are queried; and (ix)* ] *if*
81  *applicable, any other entities with which the agency shared facial recognition data.*
82      *F. Any chief of police whose agency uses facial recognition technology shall publicly post and*
83  *annually update a report by April 1 each year to provide information to the public regarding the*
84  *agency's use of facial recognition technology. The report shall include all data required by clauses (ii)*
85  *through (viii) of subsection E in addition to (i) all instances of unauthorized access of the facial*
86  *recognition technology, including any unauthorized access by employees of the agency; (ii) vendor*
87  *information, including the specific algorithms employed; and (iii) if applicable, data or links related to*
88  *third-party testing of such algorithms, including any reference to variations in demographic*
89  *performance. If any information or data (a) contains an articulable concern for any person's safety, (b)*
90  *is otherwise prohibited from public disclosure by federal or state statute, or (c) if disclosed, may*
91  *compromise sensitive criminal justice information, such information or data may be excluded from*
92  *public disclosure. Nothing herein shall limit disclosure of data collected pursuant to subsection E when*
93  *such disclosure is related to a writ of habeas corpus.*
94      *For purposes of this subsection, "sensitive criminal justice information" means information related to*
95  *(1) a particular ongoing criminal investigation or proceeding, (2) the identity of a confidential source,*
96  *or (3) law-enforcement investigative techniques and procedures.*
97      *G. At least 30 days prior to procuring facial recognition technology, a local law-enforcement agency*
98  *shall notify in writing the governing body of the locality that such agency serves of such intended*
99  *procurement, but such notice shall not be required if such procurement is directed by the governing*
100  *body.*
101      *H.* Nothing in this section shall apply to commercial air service airports.
102      [ *I. Any facial recognition technology operator employed by a local law-enforcement agency who (i)*
103  *violates the agency's policy for the use of facial recognition technology or (ii) conducts a search for any*
104  *reason other than an authorized use is guilty of a Class 3 misdemeanor and shall be required to*
105  *complete training on the agency's policy on and authorized uses of facial recognition technology before*
106  *being reinstated to operate such facial recognition technology. The local law-enforcement agency shall*
107  *terminate from employment any facial recognition technology operator who violates clause (i) or (ii) for*
108  *a second time.* ]
109      **§ 23.1-815.1. Facial recognition technology; approval [ ; penalty ] .**
110      A. For purposes of this subsection, "facial *section:*
111      *"Authorized use" means the use of facial recognition technology to (i) help identify an individual*
112  *when there is a reasonable suspicion the individual has committed* [ *, is committing, or is planning the*
113  *commission of* ] *a crime; (ii) help identify a crime victim, including a victim of online sexual abuse*
114  *material; (iii) help identify a person who may be a missing person or witness to criminal activity; (iv)*
115  *help identify a victim of human trafficking or an individual involved in the trafficking of humans,*
116  *weapons, drugs, or wildlife; (v) help identify an online recruiter of criminal activity, including but not*
117  *limited to human, weapon, drug, and wildlife trafficking; (vi) help a person who is suffering from a*
118  *mental or physical disability impairing* [ *the person's his* ] *ability to communicate and be understood;*
119  *(vii) help identify a deceased person; (viii) help identify a person who is incapacitated or otherwise*
120  *unable to identify himself; (ix) help identify a person who is reasonably believed to be a danger to*
121  *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;*
123 *(xii) ensure officer safety as part of the vetting of undercover law enforcement; (xiii) determine whether*
124 *an individual may have unlawfully obtained one or more state driver's licenses, financial instruments, or*
125 *other official forms of identification using information that is fictitious or associated with a victim of*
126 *identity theft; or (xiv) help identify a person who an officer reasonably believes is concealing his true*
127 *identity and about whom the officer has a reasonable suspicion has committed a crime other than*
128 *concealing his 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~~
131 ~~photos, videos, or real time~~ *conducting an algorithmic comparison of images of a person's facial*
132 *features for the purpose of identification.* "Facial recognition technology" does not include the use of an
133 automated or semi-automated process to redact a recording in order to protect the privacy of a subject
134 depicted in the recording prior to release or disclosure of the recording outside of the law-enforcement
135 agency if the process does not generate or result in the retention of any biometric data or surveillance
136 information.
137 *"Publicly post" means to post on a website that is maintained by the entity or on any other website*
138 *on which the entity generally posts information and that is available to the public or that clearly*
139 *describes how the public may access such data.*
140 *"State Police Model Facial Recognition Technology Policy" means the model policy developed and*
141 *published by the Department of State Police pursuant to § 52-4.5.*
142 B. ~~No~~ *Pursuant to § 2.2-1112, the Division of Purchases and Supply (the Division) shall determine*
143 *the appropriate facial recognition technology for use in accordance with this section. The Division shall*
144 *not approve any facial recognition technology unless it has been evaluated by the National Institute of*
145 *Standards and Technology (NIST) as part of the Face Recognition Vendor Test. Any facial recognition*
146 *technology utilized shall utilize algorithms that have demonstrated (i) an accuracy score of at least 98*
147 *percent true positives within one or more datasets relevant to the application in a NIST Facial*
148 *Recognition Vendor Test report, and (ii) minimal performance variations across demographics*
149 *associated with race, skin tone, ethnicity, or gender. The Division shall require all approved vendors to*
150 *annually provide independent assessments and benchmarks offered by NIST to confirm continued*
151 *compliance with this section.*
152 *C. A* campus police department ~~shall~~ ~~purchase~~ ~~or~~ ~~deploy~~ *may use* facial recognition technology ~~unless~~
153 ~~such~~ ~~purchase~~ ~~or~~ ~~deployment~~ ~~of~~ ~~facial~~ ~~recognition~~ ~~technology~~ ~~is~~ ~~expressly~~ ~~authorized~~ ~~by~~ ~~statute~~ *for*
154 *authorized uses.* ~~For~~ ~~purposes~~ ~~of~~ ~~this~~ ~~section,~~ ~~a~~ ~~statute~~ ~~that~~ ~~does~~ ~~not~~ ~~refer~~ ~~to~~ ~~facial~~ ~~recognition~~
155 ~~technology~~ ~~shall~~ ~~not~~ ~~be~~ ~~construed~~ ~~to~~ ~~provide~~ ~~express~~ ~~authorization.~~ ~~Such~~ ~~statute~~ ~~shall~~ ~~require~~ ~~that~~ ~~any~~
156 ~~facial~~ ~~recognition~~ ~~technology~~ ~~purchased~~ ~~or~~ ~~deployed~~ ~~by~~ ~~the~~ ~~campus~~ ~~police~~ ~~department~~ ~~be~~ ~~maintained~~
157 ~~under~~ ~~the~~ ~~exclusive~~ ~~control~~ ~~of~~ ~~such~~ ~~campus~~ ~~police~~ ~~department~~ ~~and~~ ~~that~~ ~~any~~ ~~data~~ ~~contained~~ ~~by~~ ~~such~~ ~~facial~~
158 ~~recognition~~ ~~technology~~ ~~be~~ ~~kept~~ ~~confidential,~~ ~~not~~ ~~be~~ ~~disseminated~~ ~~or~~ ~~resold,~~ ~~and~~ ~~be~~ ~~accessible~~ ~~only~~ ~~by~~ ~~a~~
159 ~~search~~ ~~warrant~~ ~~issued~~ ~~pursuant~~ ~~to~~ ~~Chapter~~ ~~5~~ ~~(§~~ ~~19.2-52~~ ~~et~~ ~~seq.)~~ ~~of~~ ~~Title~~ ~~19.2~~ ~~or~~ ~~an~~ ~~administrative~~ ~~or~~
160 ~~inspection~~ ~~warrant~~ ~~issued~~ ~~pursuant~~ ~~to~~ ~~law.~~ *A match made through facial recognition technology shall not*
161 *constitute probable cause for an arrest but shall be admissible as exculpatory evidence.*
162 *D. A campus police department shall publicly post its policy on use of facial recognition technology*
163 *before employing such facial recognition technology to investigate a specific criminal incident or citizen*
164 *welfare situation. A campus police department that uses facial recognition technology may adopt the*
165 *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*
169 *policy. Any policy adopted or developed pursuant to this subsection shall be updated annually.*
170 *E. Any campus police department that uses facial recognition technology shall maintain records*
171 *sufficient to facilitate discovery in criminal proceedings, post-conviction proceedings, public reporting,*
172 *and auditing of compliance with such department's facial recognition technology policies. Such*
173 *department that uses facial recognition technology shall collect data pertaining to (i) a complete history*
174 *of each user's queries; (ii) the total number of queries conducted; (iii) the number of queries that*
175 *resulted in a list of possible candidates; (iv) how many times an examiner offered campus police an*
176 *investigative lead based on his findings; (v) how many cases were closed due to an investigative lead*
177 *from facial recognition technology; (vi) what types of criminal offenses are being investigated; (vii) the*
178 *nature of the image repository being compared or queried;* [ ~~and~~ ] *(viii)* [ *demographic information for*
179 *the individuals whose images are queried; and (ix)* ] *if applicable, any other entities with which the*
180 *department shared facial recognition data.*
181 *F. Any chief of a campus police department whose agency uses facial recognition technology shall*
182 *publicly post and annually update a report by April 1 each year to provide information to the public*

183 *regarding the agency's use of facial recognition technology. The report shall include all data required*
184 *by clauses (ii) through (viii) of subsection E in addition to (i) all instances of unauthorized access of the*
185 *facial recognition technology, including any unauthorized access by employees of the campus police*
186 *department; (ii) vendor information, including the specific algorithms employed; and (iii) if applicable,*
187 *data or links related to third-party testing of such algorithms, including any reference to variations in*
188 *demographic performance. If any information or data (a) contains an articulable concern for any*
189 *person's safety, (b) is otherwise prohibited from public disclosure by federal or state statute, or (c) if*
190 *disclosed, may compromise sensitive criminal justice information, such information or data may be*
191 *excluded from public disclosure. Nothing herein shall limit disclosure of data collected pursuant to*
192 *subsection E when such disclosure is related to a writ of habeas corpus.*
193     *For purposes of this subsection, "sensitive criminal justice information" means information related to*
194 *(1) a particular ongoing criminal investigation or proceeding, (2) the identity of a confidential source,*
195 *or (3) law-enforcement investigative techniques and procedures.*
196     *G. At least 30 days prior to procuring facial recognition technology, a campus police department*
197 *shall notify in writing the institution of higher education that such department serves of such intended*
198 *procurement, but such notice shall not be required if such procurement is directed by the governing*
199 *body.*
200     [ *H. Any facial recognition technology operator employed by a campus police department who (i)*
201 *violates the department's policy for the use of facial recognition technology or (ii) conducts a search for*
202 *any reason other than an authorized use is guilty of a Class 3 misdemeanor and shall be required to*
203 *complete training on the department's policy on and authorized uses of facial recognition technology*
204 *before being reinstated to operate such facial recognition technology. The campus police department*
205 *shall terminate from employment any facial recognition technology operator who violates clause (i) or*
206 *(ii) for a second time.* ]
207     *§ 52-4.5. Department to establish a State Police Model Facial Recognition Technology Policy.*
208     *The Department shall create a model policy regarding the use of facial recognition technology,*
209 *which shall be known as the State Police Model Facial Recognition Technology Policy. The Department*
210 *shall publicly post such policy no later than January 1, 2023, and such policy shall be updated annually*
211 *thereafter and shall include:*
212     *1. The nature and frequency of specialized training required for an individual to be authorized by a*
213 *law-enforcement agency to utilize facial recognition as authorized by this section;*
214     *2. The extent to which a law-enforcement agency shall document (i) instances when facial*
215 *recognition technology is used for authorized purposes and (ii) how long such information is retained;*
216     *3. Procedures for the confirmation of any initial findings generated by facial recognition technology*
217 *by a secondary examiner; and*
218     *4. Promulgation of standing orders, policies, or public materials by law-enforcement agencies that*
219 *use facial recognition technology.*
220     *For purposes of this section, "publicly post" shall have the same meaning as defined in*
221 *§ 15.2-1723.2.*
222 **[ 2. That the Virginia State Crime Commission (the Crime Commission) shall analyze and report**
223 **on the usage data of facial recognition technology reported and published by local**
224 **law-enforcement agencies and campus police departments pursuant to the provisions of this act.**
225 **The Crime Commission shall include in its report an analysis of and recommendations for (i)**
226 **improving the use of facial recognition technology as it relates to demographics associated with**
227 **race, skin tone, ethnicity, and gender; (ii) specialized training, data storage, data retention, and the**
228 **use of a second examiner pursuant to the State Police Model Facial Recognition Technology Policy**
229 **established by § 52-4.5 of the Code of Virginia, as created by this act; and (iii) investigations and**
230 **investigative outcomes related to the accuracy of identification across different demographic**
231 **groups. The Crime Commission shall submit its report to the Chairmen of the Senate Committee**
232 **on the Judiciary and the House Committee on Public Safety by November 1, 2025. ]**
233 **[ 3. That the provisions of this act shall expire on July 1, 2026. ]**
234