22106576D

SENATE BILL NO. 741

FLOOR AMENDMENT IN THE NATURE OF A SUBSTITUTE

(Proposed by Senator McDougle

on February 14, 2022)

(Patron Prior to Substitute—Senator Surovell)

A BILL to amend and reenact § 15.2-1723.2 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 of the Code of Virginia is 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~~*:*

"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 Face Recognition Vendor Test report and (ii) 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 that is an act of violence as defined in § 19.2-297.1, identifying a victim of online child sexual abuse material, or identifying a deceased person*. ~~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 any use of 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 and may not be used as evidence by the Commonwealth during its case-in-chief in any prosecution but shall be admissible as exculpatory evidence. No evidence discovered or obtained as the result of a match in violation of this section, including any evidence subsequently discovered or obtained after such match has been made, shall be admissible in any trial, hearing, or other proceeding.

D. Prior to the use of use facial recognition technology for investigating a specific criminal incident, a law-enforcement officer shall apply for a search warrant from a judicial officer to permit the use of such facial recognition technology. Each application for a search warrant authorizing the use of facial recognition technology shall be made in writing, upon oath or affirmation, to a judicial officer for the circuit in which the facial recognition technology is to be used.

The law-enforcement officer shall submit an affidavit, which may be filed by electronically

transmitted (i) facsimile process or (ii) electronic record as defined in § 59.1-480, and shall include:

1. The identity of the applicant and the identity of the law-enforcement agency conducting the investigation;

2. Material facts constituting the probable cause for the issuance of the search warrant and alleging substantially the offense in relation to which such facial recognition technology is to be used and a showing that probable cause exists that the information likely to be obtained will be evidence of the commission of such offense or will identify a person involved in or connected to such offense; and

3. The name of the county or city where there is probable cause to believe the offense for which the facial recognition technology is sought has been committed, is being committed, or will be committed.

If the judicial officer finds, based on the affidavit submitted, that there is probable cause to believe that a crime has been committed, is being committed, or will be committed and that there is probable cause to believe the information likely to be obtained from the use of the facial recognition technology will be evidence of the commission of such offense or will identify a person involved in or connected to such offense, the judicial officer shall issue a search warrant authorizing the use of the facial recognition technology. The search warrant shall authorize the use of the facial recognition technology from within the Commonwealth, not to exceed 15 days from the issuance of the search warrant. The circuit court may, for good cause shown, grant one or more extensions, not to exceed 15 days each.

The affidavit shall be certified by the judicial officer who issues the search warrant and shall be delivered to and preserved as a record by the clerk of the circuit court of the county or city where there is probable cause to believe the offense for which the use of facial recognition technology has been sought. The affidavit shall be delivered by the judicial officer or his designee or agent in person; mailed by certified mail, return receipt requested; or delivered by electronically transmitted facsimile process or by use of filing and security procedures as defined in the Uniform Electronic Transactions Act (§ 59.1-479 et seq.) for transmitting signed documents.

By operation of law, the affidavit, search warrant, return, and any other related materials or pleadings shall be sealed. Upon motion of the Commonwealth or the person who was the subject of the facial recognition technology, the circuit court may unseal such documents if it appears that the unsealing is consistent with the ends of justice or is necessary to reasonably inform such person of the nature of the evidence to be presented against him or to adequately prepare for his defense.

The search warrant shall command the law-enforcement officer to complete the use of the facial recognition technology by the search warrant within 15 days after issuance of the search warrant. The law-enforcement officer executing the search warrant shall enter on it the exact date and time the facial recognition technology was used and the period during which it was used. Within 10 days after the use of the facial recognition technology has ended, the executed search warrant shall be returned to the circuit court of the county or city where there is probable cause to believe the offense for which the facial recognition technology has been sought has been committed, is being committed, or will be committed, as designated in the search warrant, where it shall be preserved as a record by the clerk of the circuit court.

Within 10 days after the use of the use of the facial recognition technology has ended, a copy of the executed search warrant shall be served on the person who was the subject of the facial recognition technology. Service may be accomplished by delivering a copy to such person by leaving a copy with any person found at the person's usual place of abode who is a member of the person's family, other than a temporary sojourner or guest, and who is 16 years of age or older and by mailing a copy to the person's last known address. Upon request, and for good cause shown, the circuit court may grant one or more extensions for such service for a period not to exceed 30 days each. Good cause shall include a continuing criminal investigation, the potential for intimidation, the endangerment of an individual, or the preservation of evidence.

~~C.~~ *E. 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.*

F. 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.

G. 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 F 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 is prohibited from public disclosure by federal or state statute, such information or data may be excluded from public disclosure.

H. 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.

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

J. It shall be unlawful for any person having or acquiring access to facial recognition technology that is governed by the provisions of this section to willfully use such facial recognition technology in violation of this section. Any person who willfully uses such facial recognition technology in violation of this section is guilty of a Class 2 misdemeanor.

§ 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.