22102155D

HOUSE BILL NO. 1339

Offered January 21, 2022

A BILL to amend and reenact §§ 15.2-1723.2 and 23.1-815.1 of the Code of Virginia, relating to facial recognition technology; local law enforcement; campus police.

Patrons—Leftwich; Senator: Surovell

Referred to Committee on Public Safety

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 as follows:

§ 15.2-1723.2. Facial recognition technology; approval.

A. For purposes of this section, "facial recognition technology" means an electronic system 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 an individual's facial features for the purposes of verification or 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.

B. ~~No local law-enforcement agency shall purchase or deploy facial recognition technology unless such purchase or deployment of facial recognition technology is expressly authorized by statute. 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 local law-enforcement agency may utilize facial recognition technology for criminal investigative and administrative investigative purposes. The following criteria apply to the lawful use of facial recognition technology under this subsection:

1. Any facial recognition technology used shall have been evaluated by the National Institute of Standards and Technology and received an accuracy score of 98 percent or better for true positives across all demographic groups in the Face Recognition Vendor Test.

2. The match of an image by facial recognition technology shall not constitute probable cause for arrest of an individual. The match of an image by facial recognition technology shall be permitted as exculpatory evidence.

3. A local law-enforcement agency may use facial recognition technology to search against any publicly available or lawfully acquired image or image database.

C. No later than January 1, 2023, the Department of State Police, in consultation with stakeholder organizations, shall develop and publicly post a model policy regarding the investigative use of facial recognition technology. Such model policy shall be updated at least annually and address the following subjects:

1. Training: the nature and frequency of specialized training required to authorize Virginia law-enforcement agency personnel to utilize facial recognition technology for criminal investigative and administrative investigative purposes.

2. Transparency: the extent to which a Virginia law-enforcement agency shall document instances when facial recognition technology is utilized for criminal investigative and administrative investigative purposes and how long such documentation must be retained.

3. Responsibility: whether the initial findings generated by facial recognition technology for criminal investigative and administrative investigative purposes must be confirmed by a secondary examiner.

D. A local law-enforcement agency shall publicly post the policies that will govern its use prior to utilizing facial recognition technology for criminal investigative and administrative investigative purposes. A local law-enforcement agency may adopt the model policy developed by the Department of State Police pursuant to subsection C or develop its own policy that addresses the subjects identified in subsection C. Any policy developed and adopted by a local law-enforcement agency shall be updated at least annually.

E. A local law-enforcement agency utilizing facial recognition technology shall maintain records sufficient to facilitate public reporting and auditing of compliance with the agency's facial recognition policies. Specifically, any law-enforcement agency utilizing facial recognition technology shall collect data and information pertaining to (i) the total number of system queries conducted, (ii) the number of queries that resulted in the facial recognition system offering potential candidates, (iii) the number of times an examiner offered an investigative lead for follow-up based on his findings, (iv) the number of cases closed by arrest where a facial recognition investigative lead was a contributing factor, (v) the suspected criminal offenses being investigated, (vi) the image repository searched, and (vii) records detailing any other entities that received facial recognition data shared by the agency.

F. The head of any local law-enforcement agency utilizing facial recognition technology shall be responsible for publishing an annual report by April 1 of the following year, in print or on a publicly accessible website, to provide information to the community regarding the agency's use of facial recognition technology. The report shall include data required by subsection E. Exceptions to public disclosure are only authorized for specific information if there is an articulable concern for any person's safety, if information is otherwise prohibited from public disclosure by federal or state statute, or if sensitive criminal justice information may be compromised as a result of the disclosure. Any data breaches or unauthorized access of the facial recognition system, including by agency employees, shall be disclosed in the report. Additionally, vendor information, to include the specific algorithms utilized shall be included in the report. Data or links to third-party testing of algorithms in use shall be provided, to include any reference to demographic performance variation.

G. No local government may prohibit or further restrict the use of facial recognition technology by local law-enforcement agencies.

~~C.~~ *H.* 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, "facial recognition technology" means an electronic system 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 an individual's facial features for the purposes of verification or 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.

B. ~~No campus police department shall purchase or deploy facial recognition technology unless such purchase or deployment of facial recognition technology is expressly authorized by statute. 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 campus police department may utilize facial recognition technology for criminal investigative and administrative investigative purposes. The following criteria apply to the lawful use of facial recognition technology under this subsection:

1. Any facial recognition technology used shall have been evaluated by the National Institute of Standards and Technology and received an accuracy score of 98 percent or better for true positives across all demographic groups in the Face Recognition Vendor Test.

2. The match of an image by facial recognition technology shall not constitute probable cause for arrest of an individual. The match of an image by facial recognition technology shall be permitted as exculpatory evidence.

4. A campus police department may use facial recognition technology to search against any publicly available or lawfully acquired image or image database.

C. A campus police department shall publicly post the policies that will govern its use prior to utilizing facial recognition technology for criminal investigative and administrative investigative purposes. A campus police department may adopt the model policy developed by the Department of State Police pursuant to Chapter 17 (§ 15.2-1723.2 et seq.) of Title 15.2 or develop its own policy that addresses the subjects identified in that section. Any policy developed and adopted by a campus police department shall be updated at least annually.

D. A campus police department utilizing facial recognition technology shall maintain records sufficient to facilitate public reporting and auditing of compliance with the agency's facial recognition policies. Specifically, any campus police department utilizing facial recognition technology shall collect data and information pertaining to (i) the total number of system queries conducted; (ii) the number of

queries that resulted in the facial recognition system offering potential candidates; (iii) the number of times an examiner offered an investigative lead for follow-up based on his findings; (iv) the number of cases closed by arrest where a facial recognition investigative lead was a contributing factor; (v) the suspected criminal offenses being investigated; (vi) the image repository searched; and (vii) records detailing any other entities that received facial recognition data shared by the department.

E. The head of any campus police department utilizing facial recognition technology shall be responsible for publishing an annual report by April 1 of the following year, in print or on a publicly accessible website, to provide information to the community regarding the department's use of facial recognition. The report shall include data required by subsection E. Exceptions to public disclosure are only authorized for specific information if there is an articulable concern for any person's safety, if information is otherwise prohibited from public disclosure by federal or state statute, or if sensitive criminal justice information may be compromised as a result of the disclosure. Any data breaches or unauthorized access of the facial recognition system, including by agency employees, shall be disclosed in the report. Additionally, vendor information, to include the specific algorithms utilized shall be included in the report. Data or links to third-party testing of algorithms in use shall be provided, to include any reference to demographic performance variation.

F. No local government may prohibit or further restrict the use of facial recognition technology by campus police departments.