

Department of Legislative Services

Maryland General Assembly

2017 Session

FISCAL AND POLICY NOTE

First Reader

House Bill 1148

(Delegate Sydnor)

Judiciary

Face Recognition Act

This bill establishes procedures for the use of images and information for “face recognition” and authorizes a court to issue an order authorizing the use of face recognition. “Face recognition” means the automated or semiautomated process by which an individual is sought to be identified based on the characteristics of the individual’s face, including irises and ears. The bill (1) prohibits the use of face recognition under specified circumstances; (2) requires the Department of Public Safety and Correctional Services (DPSCS) and specified law enforcement agencies to adopt an audit process to ensure that face recognition is used only for legitimate law enforcement purposes; (3) requires disclosure of specified information regarding the use of face recognition; and (4) provides for discovery related to face recognition and “appropriate relief” for a violation of the bill’s provisions.

Fiscal Summary

State Effect: Potential significant increase in State expenditures for DPSCS to create a new system or hire additional staff to meet the bill’s tracking, auditing, and reporting requirements. Potential minimal increase in general fund revenues and expenditures due to the bill’s penalty provision. The bill is not expected to have a significant fiscal impact on the Judiciary, the Motor Vehicle Administration (MVA), the Department of State Police (DSP), or other State law enforcement agencies.

Local Effect: Local expenditures may increase significantly for local law enforcement agencies that use face recognition to meet the bill’s tracking, auditing, and reporting requirements. Potential minimal increase in local revenues and expenditures due to the bill’s penalty provision. **This bill imposes a mandate on a unit of local government.**

Small Business Effect: None.

Analysis

Bill Summary:

Face Recognition Use: A police officer may not use or request targeted face recognition in conjunction with an arrest photo database unless that officer (1) has probable cause to believe that the individual the police officer seeks to identify has committed, is committing, or is about to commit a misdemeanor or a felony and (2) documents that probable cause before or immediately after the use or request.

A police officer may not use or request targeted face recognition in conjunction with a State identification photo database without a court order. A police officer also may not use or request continuous face recognition without a court order.

Issuance of Order: A court may issue an order relating to targeted face recognition in conjunction with a State identification photo database by application on a determination that there is probable cause to believe that (1) a misdemeanor or felony has been, is being, or will be committed by the individual sought to be identified and (2) the use of face recognition will lead to evidence of the misdemeanor or felony being investigated or the apprehension of an individual against whom an arrest warrant has been issued previously.

A court may issue an order relating to continuous face recognition in conjunction with an emergency watch list by application on a determination that there is probable cause to believe that (1) a felony involving the immediate danger of death or serious bodily injury has been, is being, or will be committed by the individual or individuals included in the emergency watch list; (2) an emergency situation exists that requires the use of continuous face recognition without delay; and (3) the use of face recognition will lead to evidence of the felony being investigated or apprehension of an individual for whom an arrest warrant has been issued previously, or prevent a death or serious bodily injury.

An application for an order must be in writing, signed and sworn to or by the applicant, and accompanied by an affidavit that sets forth the basis for probable cause and contains facts within the personal knowledge of the affiant. The order must contain specified information relating to the suspect, the database searched, the applicant, and the search time period.

If a police officer uses or requests targeted face recognition in conjunction with a State identification photo database or continuous face recognition, the officer must apply for an order approving the use within 24 hours after the use occurs or initiates. If the order is denied or the application is not made within 24 hours, the use must terminate immediately and all information obtained as a result of the search must be destroyed.

Legitimate Law Enforcement Purpose: Generally, a police officer may use or request targeted or continuous face recognition only for a legitimate law enforcement purpose. The bill lists the following circumstances under which a police officer may explicitly use or request targeted or continuous face recognition:

- in exigent circumstances;
- to identify or locate an individual who is deceased, incapacitated, or reasonably suspected to be the victim of a crime, whom the officer determines, in good faith, cannot be identified through other means;
- to locate an individual who has been reported missing, including the subject of an amber or silver alert;
- to identify an individual who has been lawfully arrested, during the process of booking that individual after an arrest or during that individual's custodial detention; or
- to assist MVA in investigating individual cases of identity fraud through deduplication analysis.

A police officer who knowingly uses or requests targeted or continuous face recognition for a purpose other than a legitimate law enforcement purpose is subject to imprisonment not exceeding one year and/or a fine not exceeding \$10,000.

Notification of Request: An individual arrested as a result of an investigative lead generated through the use or request of targeted or continuous face recognition must be notified of that use or request. The notice must (1) be delivered within 48 hours of that individual's arrest; (2) state the general nature of the law enforcement inquiry; and (3) provide to the individual specified information and a copy of the order.

Generally, the court, on a specified finding of good cause, may order that the application, affidavit, and orders issued be sealed and that the required notification be delayed for a period of 30 calendar days, or for an additional period, if the court makes a specified finding.

Discovery: Discovery of an application, affidavit, or order relating to continuous or targeted face recognition and any documents related to the use or request of continuous or targeted face recognition, if any, are subject to the Maryland Rules governing discovery in the District and circuit courts.

MVA Notice: MVA must post notices in conspicuous locations at each of its locations, make written information available to each applicant at its locations, and provide information on MVA's website regarding law enforcement face recognition searches of driver's license and identification card photographs.

Audit Process: DPSCS and any law enforcement agency using targeted or continuous face recognition must adopt an audit process to ensure that face recognition is used only for legitimate law enforcement purposes, including audits of uses or requests made by law enforcement agencies or individual police officers.

Reporting Requirements: By March 1 of each year beginning in 2018, DPSCS, in conjunction with the Maryland Coordination and Analysis Center (MCAC) and law enforcement agencies that use targeted or continuous face recognition, must report to specified legislative committees on the following information based on data from the previous calendar year, for uses or requests of targeted face recognition in conjunction with an arrest database, targeted face recognition in conjunction with a State identification photo database, and continuous face recognition in conjunction with an emergency watch list, respectively:

- the number of searches run;
- the number of arrests and convictions that resulted from the searches;
- the offenses that the searches were used to investigate;
- the number of motions to suppress made with respect to the searches;
- the number of searches run for targeted or continuous face recognition in exigent circumstances;
- for targeted face recognition in conjunction with an arrest photo database or a State identification photo database, respectively, summary statistics on the race, ethnicity, age, and gender of the individuals whose faces were searched;
- for continuous face recognition in conjunction with an emergency watch list, the following: the specific locations where the searches were run; the duration of those searches; the number of individuals included on the emergency watch list; and summary statistics on the race, ethnicity, age, and gender of the individuals included on the list; and
- a list of audits that were completed by MCAC or a law enforcement agency and a summary of the audit results.

Limitation on Use in Evidence: Except as specified, when targeted or continuous face recognition is used or requested, results from those searches and evidence derived from the targeted or continuous face recognition may not be received in evidence in a trial, a hearing, or any other proceeding in or before a court, grand jury, department, officer, agency, regulatory body, legislative committee, or any other authority of the State if the use of face recognition violated the bill's provisions or the police officer was required to subsequently obtain an order for the use or request for targeted or continuous face recognition, as specified, but did not subsequently obtain such an order.

Appropriate Relief: An individual who is subject to identification or attempted identification through targeted continuous face recognition in violation of the bill's provisions, or who does not receive a required notice, may recover "appropriate relief" in a civil action from the law enforcement agency that employs the police officer. The trier of fact may assess as damages the greater of the sum of the actual damages suffered by the plaintiff as a result of the violation or statutory damages of the greater of \$500 a day for each day of violation or \$50,000. "Appropriate relief" includes, as appropriate, preliminary and other equitable or declaratory relief, actual damages and punitive damages, and reasonable attorney's fees and other litigation costs reasonably incurred. It is a complete defense against any civil or criminal action brought under the bill's provisions if the defendant relies in good faith on a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization. A civil action may not be commenced later than three years after the date on which the claimant first has a reasonable opportunity to discover the violation.

Definitions: "Arrest photo database" means a government or private database populated primarily by booking or arrest photographs or photographs of individuals encountered by police officers.

"Continuous face recognition" means the use of face recognition on groups of individuals as part of a criminal investigation or general surveillance, including the use of face recognition to continuously identify individuals whose images are captured or recorded by a surveillance camera.

"Emergency watch list" means a highly targeted database populated by a specific individual or individuals whom there is probable cause to believe have committed, are committing, or are about to commit an offense that involves the immediate danger of death or serious physical injury to another individual.

"Legitimate law enforcement purpose" means the investigation, detection, or analysis of a crime or the operation of terrorists or missing or endangered person searches or alerts.

"State identification photo database" means a government or private database populated primarily by photographs from drivers' licenses or identification documents made or issued by or under the authority of the state.

"Targeted face recognition" means the use of face recognition to identify or attempt to identify a specific individual as part of a specific criminal investigation.

Current Law: The use and operation of face recognition is not now restricted by law in Maryland; however, access is limited for MVA records with personal information and DPSCS case records for inmates. Generally, MVA is prohibited from disclosing a public record containing personal information; however, MVA is required to disclose personal information from its public records for use by a federal, state, or local government, HB 1148/ Page 5

including a law enforcement agency, or a court in carrying out its functions. Similarly, DPSCS is prohibited from disclosing the content of an inmate case record; however, disclosure is authorized to an employee of any State unit or a federal or local law enforcement unit, if disclosure is in furtherance of the employee's lawful duties.

Background: According to the National Conference of State Legislatures, 47 states including Maryland have laws that apply to personal data, which potentially includes information gathered by facial recognition technology. The Maryland Image Repository System (MIRS) is facial recognition software within DPSCS that allows law enforcement to compare images of unidentified individuals to images from MVA records, inmate case records, and mugshots. DPSCS has been responsible for the maintenance and implementation of the system and database since 2011.

MIRS requires a digital image to be uploaded to conduct a search. The uploaded image is converted to a minutiae template; the face becomes a series of numbers. Facial recognition systems measure nodal points on the face and the measurements, via algorithm, become a minutiae template. The system searches the templates of known individuals for numbers that are close to those on the probe template. MIRS does not provide "hits" or "matches" to the probe image; instead, it provides a probability list of candidates, ranked by the highest number. Overall, DPSCS states that investigators use this information as any other image comparison is used to develop a positive identification of a suspect.

According to a 2016 U.S. Government Accountability Office [report](#), there are concerns about the accuracy of facial recognition software and the possibility of the system producing a false positive. However, DPSCS advises that MIRS only gives a probable list of potential suspects to be followed up on by law enforcement. Currently, local law enforcement agencies in the State are responsible for establishing a policy regarding the use of MIRS and decide when, where, and how it is used.

DPSCS states that only Maryland law enforcement agencies have access to MIRS and the department is able to see who logs on to the system. Similar to access to the National Crime Information Center within the Federal Bureau of Investigation, only authorized users are able to access the system as necessary to perform an authorized task. DPSCS also states that people in public places are never scanned by MIRS.

While the use of face recognition and motor vehicle data are not prohibited by law, the Center on Privacy and Technology at Georgetown Law recommends that federal and state law enforcement agencies increase transparency, audit and review procedures for such software, and ensure adherence to privacy laws. The Center has established [model legislation](#) on which this bill is based.

State Expenditures: The bill has a significant impact on DPSCS because (1) although MIRS access is limited, DPSCS does not have the capability to audit MIRS to determine

the purpose for which a police officer accesses the system; (2) DPSCS does not have the capability to ensure that the system is accessed only with probable cause or after a police officer has obtained a court order; and (3) MIRS does not capture most of the information that DPSCS is required to report under the bill. In order to meet the bill's requirements, DPSCS either needs to hire additional staff to follow up each time the system is accessed or create a new system and obtain additional storage. DPSCS advises that it is unable to determine the cost of a new system or the number of additional staff that might be needed to meet the bill's requirements. However, in either case, general fund expenditures increase significantly.

The bill may result in an increase in workload for the Judiciary to prepare new forms and handle additional hearings for petitions of orders; it is assumed that any such increase can be handled with existing budgeted resources. The bill is not anticipated to significantly affect the finances of MVA, DSP, or other State law enforcement agencies.

Local Expenditures: The bill's tracking, auditing, and reporting requirements increase workloads for some jurisdictions that use MIRS, which may result in the need for additional staff. Accordingly, local expenditures increase, potentially significantly, for those law enforcement agencies that use face recognition. For example, Montgomery County advises that additional administrative staff are necessary to meet the bill's tracking and reporting requirements.

Additional Information

Prior Introductions: None.

Cross File: None.

Information Source(s): Montgomery County; Maryland Association of Counties; City of Bowie; Judiciary (Administrative Office of the Courts); Office of the Public Defender; Department of Natural Resources; Department of Public Safety and Correctional Services; Department of State Police; Maryland Department of Transportation; Military Department; National Conference of State Legislatures; U.S. Government Accountability Office; Center on Privacy and Technology at Georgetown Law; Department of Legislative Services

Fiscal Note History: First Reader - February 24, 2017
fn/lgc

Analysis by: Shirleen M. E. Pilgrim

Direct Inquiries to:
(410) 946-5510
(301) 970-5510