HB 1578

Department of Legislative Services

Maryland General Assembly
2020 Session

FISCAL AND POLICY NOTE
First Reader

House Bill 1578 (Delegate J. Lewis)
Judiciary

Facial Recognition Privacy Protection Act

This bill establishes a regulatory framework to govern the use of facial recognition services by private entities and units of State and local government in Maryland. The bill supersedes and preempts laws, ordinances, regulations, or the equivalent adopted by a political subdivision regarding the development, use, or deployment of facial recognition services.

Fiscal Summary

State Effect: General fund expenditures increase by *at least* $255,200 in FY 2021 for reprogramming and additional staff; out-year expenditures reflect annualization and elimination of one-time costs. General fund revenues may increase minimally due to the bill's penalty provisions.

(in dollars)	FY 2021	FY 2022	FY 2023	FY 2024	FY 2025
Revenues	$0	$0	$0	$0	$0
GF Expenditure	255,200	212,900	217,900	225,400	233,200
Net Effect	($255,200)	($212,900)	($217,900)	($225,400)	($233,200)

Note:() = decrease; GF = general funds; FF = federal funds; SF = special funds; - = indeterminate increase; (-) = indeterminate decrease

Local Effect: The bill has an operational impact on local law enforcement agencies; some local law enforcement agencies may incur additional costs to comply with the bill's requirements. Local revenues are likely not affected.

Small Business Effect: Potential meaningful.

Analysis

Bill Summary: The bill establishes numerous definitions related to the use of facial recognition software and services, including the following:

- "Controller" means a person that, alone or jointly with others, determines the purpose and means of the processing of personal data.
- "Processor" means a person that processes personal data on behalf of a controller (but does not include a unit of State or local government).

The bill's requirements do not restrict the ability of a controller or processor to (1) comply with applicable laws or regulations; (2) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons; and (3) investigate, establish, exercise, prepare for, or defend legal claims.

General Requirements for the Use of Facial Recognition Services

The bill establishes numerous requirements for processors who sell and/or provide facial recognition services Broadly, the bill requires (1) each processor to ensure a controller or third party is able to conduct legitimate, independent, and reasonable tests of the facial recognition service, as specified; (2) each processor to provide documentation to an independent tester that enables the service to be tested and explains the service's capabilities and limitations; and (3) the contract that allows the use of a facial recognition service to prohibit the use of the service to unlawfully discriminate against individuals or groups of individuals.

The bill also establishes numerous requirements for controllers that obtain facial recognition services from processors to collect data, images, and facial templates. Broadly, a controller must:

- notify the general public when the service is being used in a physical premises open to the public, as specified;
- obtain consent from an individual before enrolling the individual's image or facial template into the system (except when the enrollment is done for a security or safety purpose and the data collected is maintained in a specified manner);
- ensure decisions that produce legal or similarly significant effects concerning individuals (as defined by the bill) are subject to meaningful human review;
- test the service in operational conditions before implementing it and take commercially reasonable steps to ensure best-quality results, as specified; and
- conduct periodic training that meets specified requirements for all individuals who operate the service or process personal data obtained from it.

Additionally, a controller may not knowingly disclose personal data obtained from a facial recognition service to a law enforcement agency unless the disclosure is made in a specified manner or meets other specified requirements.

Rights and Protections for Individuals

The bill establishes various protections and rights for individuals whose data, images, and facial templates are collected and stored by a facial recognition service. Broadly, an individual has the right to have an image or facial template of the individual removed from the system, except under specified circumstances and withdraw consent to enroll an image or facial template into the service.

An individual may exercise any such right by submitting a request, at any time, to a controller specifying which rights the individual wishes to exercise. A controller must generally comply with a request and respond within a specified timeframe, and a processor must assist the controller with compliance, as specified. The bill establishes the circumstances under which a controller may refuse to act on a request or charge a reasonable fee to cover the costs of complying with the request.

Requirements for Units of State and Local Government

The bill establishes various rules and requirements that must be followed by any unit of State or local government that uses or intends to develop, procure, or use a facial recognition service. Broadly, a unit of State or local government that does so must:

- produce an accountability report (and update it every two years) for the service that, among other things, includes the type or types of data being collected, the purposes and proposed use for the data being collected (including any related benefits), and a use and data management policy that meets specified requirements;
- seek public comment under specified circumstances;
- prepare an annual report disclosing specified information about the use of the service, submit the report to the Department of Information Technology (DoIT), and hold a community meeting to review the report at least 60 days before its submission;
- ensure decisions that produce legal or similarly significant effects concerning individuals (as defined by the bill) are subject to meaningful human review;
- test the service in operational conditions before implementing it and take commercially reasonable steps to ensure best-quality results, as specified;
- conduct periodic training that meets specified requirements for all individuals who operate the service or process personal data obtained from it; and

- maintain records of its use of the service sufficient to facilitate public reporting and auditing of compliance, as specified.

A unit of State or local government is prohibited from:

- using a facial recognition service to engage in ongoing surveillance unless the use is in support of law enforcement activities *and* meets other specified requirements, including obtaining a search warrant;
- applying the service to any individual based on specified characteristics (such as race, sexual orientation, religious views, political views, *etc*.), except under specified circumstances; and
- using the service to create a record describing any individual's exercise of First Amendment rights, except under specified circumstances.

If a unit of State or local government is using a facial recognition service on a criminal defendant, the unit must disclose the use to the defendant in a timely manner before trial.

By January 31 of each year, each judge who takes actions regarding warrants for ongoing surveillance under a facial recognition service must report specified information about the warrants to the Court of Appeals.

Enforcement

The Office of the Attorney General has exclusive authority to enforce the bill's requirements and prohibitions relating to controllers and processors by bringing an action in the name of the State, or as *parens patriae* on behalf of individuals residing in the State. A controller or processor that violates the bill's requirements may be subject to an injunction and liable for a civil penalty of (1) up to $2,500 for each unintentional violation and (2) $7,500 for each intentional violation.

Current Law/Background: According to news reports, local law enforcement agencies have used facial recognition software to varying degrees in recent years. For example, the Maryland Image Repository System (MIRS) is facial recognition software within the Department of Public Safety and Correctional Services (DPSCS) that allows law enforcement to compare images of unidentified individuals to images from Motor Vehicle Administration records, inmate case records, and mugshots. People in public places are never scanned by MIRS. MIRS only gives a probable list of potential suspects to be followed up on by law enforcement, not a positive identification. 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. The Anne Arundel County Police Department (AAPD) used MIRS to identify the suspected gunman at the *Capital Gazette* shooting that killed five people. AAPD used MIRS because the fingerprint identification system was operating slowly and the suspect did not have identification and refused to communicate with officers. The suspect's image was contained in MIRS because of a prior charge and conviction. The Baltimore City Police Department also reportedly used facial recognition software to identify individuals during the protests after the death of Freddie Gray.

The use of facial recognition in law enforcement investigations is also attracting national attention. In October 2019, California became the third state to ban biometric surveillance technology, including facial recognition software, in body cameras. The law, which went into effect on January 1, 2020, and remains in effect for three years, also prohibits running previously obtained body camera footage through biometric surveillance technology.

Critics of the use of facial recognition technology point out that, although law enforcement has had access to facial recognition tools for many years, it has generally relied on images from government databases, rather than private entities. However, as the technology has improved, private companies have been able to offer products that use facial recognition technology for virtually any database of images.

State/Local Fiscal Effect: DPSCS advises that, while it provides access to MIRS, it does not review or otherwise audit the law enforcement/criminal justice agencies that may voluntarily seek to use the system. Assuming DPSCS must provide reports that include a high level of detail regarding how MIRS is used by numerous State and local law enforcement agencies throughout the State, additional personnel are necessary to implement the bill's requirements.

General fund expenditures for DPSCS increase by $255,153 in fiscal 2021, which accounts for the bill's October 1, 2020 effective date. This estimate reflects the cost of hiring two program administrators and one office clerk to manage the agency's responsibilities under the bill. It includes salaries, fringe benefits, one-time start-up costs, and ongoing operating expenses. The estimate also includes one-time reprogramming costs as well as the development of training procedures and materials.

Positions	3.0
Salaries and Fringe Benefits	$164,054
Reprogramming	50,000
Development of Training Materials/Procedures	25,000
Operating Expenses	16,099
Total FY 2021 DPSCS Expenditures	**$255,153**

Future year expenditures reflect full salaries with annual increases and employee turnover and ongoing operating expenses.

Judiciary

If a facial recognition service is used to engage in ongoing surveillance, the State or local agency must obtain a search warrant through the courts. The bill's reporting requirement for all judges (to the Court of Appeals) on warrants for ongoing surveillance approved, extended, or denied in the prior year has an operational impact on the Judiciary. As it is unclear whether the process for such reporting can be automated, this analysis assumes that the reporting requirement is handled manually, which may necessitate significant staff time (but does not necessarily require additional expenditures). To the extent that the Judiciary is able to develop an automated tracking process, reprogramming costs are incurred. The Judiciary advises these costs could total as much as $93,800 in fiscal 2021.

Other Units of State and Local Government

Other State agencies are affected as well, including the Department of State Police (DSP) and the Maryland Department of Transportation (MDOT). To the extent any State law enforcement agencies use facial recognition technology while engaging in ongoing surveillance, they must obtain warrants to do so. Although MDOT is unable to quantify the fiscal impact of the bill at this time, operations are affected, as the agency must produce and install the required notices; hold public meetings; develop, implement, and carry out the required training; and produce reports. DSP advises that it already maintains detailed procedures governing the use of MIRS and can likely handle the *reporting* requirements with existing resources; however, the Department of Legislative Services advises that other requirements may affect operations or costs. In addition, DoIT advises it can handle the bill's requirement to post State and local government annual reports on its website with existing budgeted resources.

The impact on local law enforcement agencies depends on a variety of factors, including whether and how frequently the agencies rely on the use of facial recognition technology and whether they currently obtain warrants to do so before engaging in ongoing surveillance. Although it is generally assumed that any local law enforcement agencies using facial recognition services can report on their usage with existing resources, there may be operational impacts to do so and there are likely costs associated with other requirements of the bill (as noted above).

While the bill's penalty provisions may result in additional general fund revenues, any increase is assumed to be minimal.

Small Business Effect: Any small businesses in the State whose business activities involve facial recognition services may be significantly impacted under the bill. The bill establishes numerous requirements and restrictions on how such technologies may be used.

However, the number of small businesses in the State that may be affected cannot be determined.

Additional Comments: The bill does not apply to facial recognition services used by the Legislative and Judicial branches of State government.

Additional Information

Prior Introductions: None.

Designated Cross File: SB 476 (Senator Sydnor) - Finance.

Information Source(s): Department of Information Technology; Maryland Association of Counties; Maryland Municipal League; Office of the Attorney General; Judiciary (Administrative Office of the Courts); Department of Public Safety and Correctional Services; *The Washington Post*; *The Baltimore Sun*; *The New York Times*; Department of State Police; Maryland Department of Transportation; Department of Legislative Services

Fiscal Note History: First Reader - March 11, 2020
rh/ljm

Analysis by: Eric F. Pierce and Richard L. Duncan	Direct Inquiries to: (410) 946-5510 (301) 970-5510