Department of Legislative Services

Maryland General Assembly
2020 Session

FISCAL AND POLICY NOTE
First Reader

Senate Bill 46 (Senator Lee)
Judicial Proceedings

State's Attorney - Required Disclosure - Facial Recognition and DNA Analysis and Search

This bill requires the State's Attorney in a criminal case to make a timely disclosure to the defendant if "facial recognition" or "forensic genetic genealogical DNA analysis and search" was used during the criminal investigation of the case.

Fiscal Summary

State Effect: None. The bill is procedural and does not affect State finances.

Local Effect: None. The bill is procedural and does not affect local finances.

Small Business Effect: None.

Analysis

Bill Summary: The bill defines "facial recognition" as a biometric software application capable of uniquely identifying an individual based on facial characteristics, including eyes and ears. "Forensic genetic genealogical DNA analysis and search" is the forensic genetic genealogical DNA analysis of a forensic or reference sample of biological material by a laboratory to develop a profile and the subsequent search of that profile in (1) a publicly available open data personal genomics database or (2) a direct-to-consumer genetic genealogy service.

Current Law: The activity required to be disclosed under the bill is not prohibited under statute. However, statute does contains provisions addressing admissibility of DNA and searches of the statewide DNA database, as discussed below.

Admissibility of DNA Profile

Evidence of a "DNA profile," as defined in statute, is admissible in a criminal proceeding to prove or disprove the identity of any person, so long as the party seeking to introduce the evidence notifies the other party by mail within 45 days before any criminal proceeding and provides certain information on request within specified timelines. With the exception of admissibility, these requirements do not preclude discovery under the relevant Maryland Rules upon a showing of scientific relevance to a material issue regarding the DNA profile.

Statewide DNA Database

The statewide DNA database system consists of DNA samples collected from individuals convicted of a felony, fourth-degree burglary, or breaking and entering a vehicle. DNA samples for individuals charged with a "crime of violence" or burglary or an attempt to commit those crimes are also included within the statewide database.

The State Police Crime Laboratory is required to store and maintain each DNA identification record in the statewide DNA database. Matches between evidence samples and database entries may only be used as probable cause and are not admissible at trial unless confirmed by additional testing.

A person is prohibited from performing a search of the statewide database for the purpose of the identification of an offender in connection with a crime for which the offender may be a biological relative of the individual from whom the DNA sample was acquired.

A person may not willfully test a DNA sample for information that does not relate to the authorized identification of an individual, as specified. A violation is punishable by up to five years imprisonment and/or a $5,000 fine. In addition, a person is prohibited from willfully failing to destroy a DNA sample for which notification has been sent stating that the DNA sample has been destroyed or for which destruction has been ordered. Violators are subject to imprisonment of up to one year or a maximum fine of $1,000.

The bill applies to searches of publicly available genealogical databases, not the statewide DNA database system exclusively accessible by law enforcement. Therefore, the prohibitions described above do not apply to use of genealogical databases.

Background: Genealogy databases such as GEDmatch, Ancestry.com, and 23andme allow users to research information about their ancestry and genetic background by matching their DNA against publicly available DNA profiles. However, recently, due to the cutting edge combination of DNA and genetic genealogy, the public genealogy databases have also been used to help solve criminal cases. Through genetic genealogy, detectives can cast a wide net, searching distant relatives of an unknown suspect by

analyzing the DNA submitted voluntarily to a genetic genealogy database. This allows police to create a much larger family tree than using law enforcement databases such as the Combined DNA Index System, in which an exact match is needed in most states. The use of such databases by law enforcement has generated debate about privacy and civil liberties issues. At least one company has changed its policy to allow law enforcement to access matches from DNA profiles only of site users who have opted in to share their information.

While genealogy databases have been used to solve a number of cold cases, the "Golden State Killer" case has received the most attention. The Golden State Killer, also known as the East Area Rapist and the Original Night Stalker, was believed to have committed several murders, at least 50 rapes, and multiple home burglaries throughout California in the 1970s and 1980s. His last known crime was in 1986.

Although police had the unknown killer's DNA from multiple crime scenes, the Golden State Killer cases went unsolved until 2018, when investigators entered the mystery killer's DNA into the GEDmatch genealogy database. Based on the pool of people on the genealogy website, investigators were able to build a family tree of the unknown killer's relatives, who had voluntarily submitted their DNA to the database. Investigators narrowed the search based on age, location, and other characteristics, leading them to 72-year-old Joseph DeAngelo.

As a result of the profile, investigators surveilled Mr. DeAngelo and collected his DNA from a tissue left in the trash. Investigators entered his discarded DNA back into the genealogy database and found a match, linking Mr. DeAngelo's DNA to the DNA gathered at multiple crime scenes. Mr. DeAngelo has been charged with several crimes, including 13 counts of murder spanning several counties in California.

In September 2019, the U.S. Department of Justice (DOJ) announced an interim policy on the use of forensic genetic genealogy, effective November 1, 2019. The policy applies to investigations controlled by DOJ agencies and investigations in which a federal, state, or local agency has received DOJ funding to conduct genetic genealogy searches. The policy requires law enforcement to thoroughly utilize traditional investigative techniques, including use of criminal DNA databases, before pursuing genealogical searches. Also, investigators must identify themselves as law enforcement to companies providing genealogical services and may only search profiles in services that provide explicit notice to their users and the public that law enforcement may use the service for criminal investigations. Investigators must also obtain informed consent before obtaining reference samples from third parties who may be more closely related to the donor of the forensic sample/suspect than the individual identified by the genealogical service as being a relative of the donor/suspect. The policy also requires specified collaboration between investigators, prosecutors, and law enforcement.

Facial Recognition

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 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.

Additional Information

Prior Introductions: None.

Designated Cross File: None.

Information Source(s): Judiciary (Administrative Office of the Courts); Office of the Public Defender; Maryland State's Attorneys' Association; Department of Public Safety and Correctional Services; U.S. Department of Justice; ABC News; CNN; PBSNewsHour.com; *Science Magazine;* California State Assembly; *The Baltimore Sun; The Washington Post;* American Bar Association; Department of Legislative Services

Fiscal Note History: First Reader - January 13, 2020
af/jkb

Analysis by: Amy A. Devadas

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