CHARLES E. SYDNOR III, ESQ.
Legislative District 44
Baltimore City and Baltimore County

Judicial Proceedings Committee

Joint Committees

Children, Youth, and Families

Cybersecurity, Information Technology, and Biotechnology

Ending Homelessness

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

James Senate Office Building
11 Bladen Street, Room 216
Annapolis, Maryland 21401
410-841-3612 · 301-858-3612
800-492-7122 *Ext.* 3612
Charles.Sydnor@senate.state.md.us

Testimony Regarding SB 187 – Criminal Procedure-Forensic Genetic Genealogical DNA Analysis, Searching, Regulation, and Oversight
Before the Senate Judicial Proceedings Committee
On February 4, 2021

Good afternoon Mr. Chairman, members of the Judicial Proceedings Committee.

The Maryland DNA Collection Act was originally enacted in 1994, authorizing the collection of DNA in order to "assist an official investigation of a crime; to identify human remains; to identify missing persons;" as well for other purposes. In 2008, Chapter 337 amended the Act to allow the State to collect DNA from people arrested for burglary, or violent crimes, at the time of their arrest. Chapter 337 also included a provision, Section 2-506(D), which "prohibited [a person] 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."

Maryland maintains a statewide database containing DNA collected from individuals that have been convicted of certain crimes. These crimes include felonies, fourth-degree burglary, breaking and entering a vehicle, "crimes of violence", felony burglary, or an attempt to commit a crime of violence or felony burglary.[1] The term "crime of violence" includes several specific crimes, including abduction, arson, kidnapping, manslaughter, murder, rape, carjacking, first- or second-degree sexual offense, and various types of assault.[2] Maryland is one of the few, if not only state with legislation on familial DNA searching and the first to ban the practice statewide. According to a 2017 report, this ban was obtained because stakeholders cited particular concerns with FDS (familial DNA searches) related to racial justice and 4th Amendment privacy rights and lawmakers agreed.[3]

As governments and commercial enterprises develop and create their own databases, Maryland's efforts to balance privacy and public safety have fallen behind. However, with the passage of SB 187 this will no longer be the case.

---

[1] See HB 30 (2019) Fiscal and Policy Note.
[2] *Id.*
[3] Study of Familial DNA Searching Policies and Practices: Case Study Brief Series. Department of Justice's Office of Justice Programs.

Direct-to-consumer genealogy services allow anyone to submit a sample of their DNA to learn a variety of things about their genetic makeup and ancestry. These services match the DNA of the individual against publicly available DNA profiles.[4] Recently, due to the cutting-edge combination of DNA and genetic genealogy, some public genealogy databases have also been used to help solve criminal cases. Detectives have searched with relative ease for distant relatives of an unknown suspect by analyzing the DNA submitted voluntarily to these databases.[5] This allows police to create a much larger family tree than would otherwise be possible using only law enforcement databases.

Perhaps the most well-known example of police solving a crime using DNA information from a direct-to-consumer genealogy database is the Golden State Killer case. Investigators entered DNA which the killer left at crime scenes into the GEDmatch genealogy database.[6] 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.[7] Investigators narrowed the search based on age, location, and other characteristics, leading them to a suspect who did not submit his DNA to the genealogy service.[8]

Under current law, there are a variety of people who are subject to having their DNA put into the FBI's CODIS (Combined DNA Index System) database; these are persons convicted whose expectation of privacy was diminished when they were convicted. They include millions of felons, misdemeanants and in some cases, arrestees. Legislation I introduced in the past was focused on a different class of persons; persons that no reasonable person would believe has a diminished expectation of privacy. I spoke about the person who knowingly and voluntarily delivered their DNA, as well as their relatives', to a third party. This included persons who may for whatever reason submit their DNA willingly to another recreationally, maybe it is to Ancestry.com, 23 and me, or GEDMatch. I desired to ensure these people's rights were protected and respected.

When I first began my work in this area I noted a quote from Justice Scalia. He wrote "Solving unsolved crimes is a noble objective, but it occupies a lower place in the American pantheon of noble objectives than the protection of our people from suspicionless law-enforcement searches. The Fourth Amendment must prevail."[9] SB 187 seeks to put in place a legal framework that balances privacy with the need to identify those who commit the most violent felonious crimes. SB 187 framework was built upon a foundation created by the U.S. Department of Justice (DOJ) 2019 interim policy.[10] However, SB 187 also includes guidance to when this technique may be

---

[4] *Id.*
[5] *Id*
[6] Thomas Fuller, *How a Genealogy Site Led to the Front Door of the Golden State Killer Suspect*, New York Times, retrieved from https://www.nytimes.com/2018/04/26/us/golden-state-killer.html.
[7] *Id.*
[8] *Id.*
[9] Maryland v. King, 133 S. Ct. 1958 (Scalia, J., dissenting)
[10] U.S. Department of Justice, *United States Department of Justice Interim Policy: Forensic Genetic Genealogical DNA Analysis and Searching* (2019), https://www.justice.gov/olp/page/file/1204386/download.

used, judicial oversight in some key areas, and protections for those third parties who are not suspected of crimes as well as a licensing regime for those involved in this technique.

SB 187, is in all sense of the word a compromise bill, and I am okay with that. After last session, we created a workgroup.[11] This workgroup met bi-weekly over the course of two months to talk about this topic and a bill. We had the world's leading genetic genealogist CeCe Moore speak with us and provide insight into how she uses this technique. And we had long discussions and struggled over many of the provisions in this bill. However, from this work, SB 187 was born. With that, I would like to provide my panel with the opportunity to provide testimony about the functioning of this bill. I urge the committee to vote in favor of SB 187.

[11] We invited input from representatives of the Office of Public Defender, the Maryland States Attorney Association, the Maryland State Police, the Maryland Chiefs and Sheriffs, and the ACLU. We also invited Debra JH Mathews of the Johns Hopkins University Berman Institute of Bioethics, Law Professor Erin Murphy (New York University School of Law), Law Professor Natalie Ram (University of Maryland School of Law), Law Professor and Bioethicist Sonia Suter (George Washington University School of Law), Assistant Professor of Medicine, Timothy D. O'Connor, PhD., Evolutionary Genetics (University of Maryland School of Medicine) and Innocence Project founder Attorney Barry Scheck.

UNITED STATES DEPARTMENT OF JUSTICE
INTERIM POLICY
FORENSIC GENETIC GENEALOGICAL DNA ANALYSIS AND SEARCHING

I. Purpose and Scope[1]

The purpose of this interim policy is to promote the reasoned exercise of investigative, scientific, and prosecutorial discretion in cases that involve forensic genetic genealogical DNA analysis and searching ('FGGS').[2] It provides guidance to Department agencies when formulating a thoughtful and collaborative approach to important interdisciplinary decisions in cases that utilize this investigative technique. Collaboration between investigators, laboratory personnel, and prosecutors is important because the decision to pursue FGGS may affect privacy interests, the consumption of forensic samples, and law enforcement's ability to solve violent crime.

The Department must use FGGS in a manner consistent with the requirements and protections of the Constitution and other legal authorities. Moreover, the Department must handle information and data derived from FGGS in accordance with applicable laws, regulations, policies, and procedures. When using new technologies like FGGS, the Department is committed to developing practices that protect reasonable interests in privacy, while allowing law enforcement to make effective use of FGGS to help identify violent criminals, exonerate innocent suspects, and ensure the fair and impartial administration of justice to all Americans.

The Department will continue to assess its investigative tools and techniques to ensure that its policies and practices properly reflect its law enforcement mission and its commitment to respect individual privacy and civil liberties. This interim policy establishes general principles for the use of FGGS by Department components during criminal investigations and in other circumstances that involve Department resources, interests, and equities.

The scope of this interim policy is limited to the requirements set forth herein. It does not control investigative, scientific, or prosecutorial activities or decisions not specifically addressed. The Department's individual law enforcement components may issue additional guidance that is consistent with the provisions of this interim policy.

---

[1] This interim policy provides Department components with internal guidance. It is not intended to, does not, and may not be relied upon to create any substantive or procedural rights or benefits enforceable at law or in equity by any party against the United States or its departments, agencies, entities, officers, employees, agents, or any other person in any matter, civil or criminal. This interim policy does not impose any legal limitations on otherwise lawful investigative or prosecutorial activities or techniques utilized by the Department of Justice, or limit the prerogatives, choices, or decisions available to, or made by, the Department in its discretion.

[2] As used in this interim policy, the term 'forensic genetic genealogical DNA analysis and searching,' or 'FGGS,' means the forensic genetic genealogical DNA analysis of a forensic or reference sample of biological material by a vendor laboratory to develop an FGG profile and the subsequent search of that profile in a publicly-available open-data personal genomics database or a direct-to-consumer genetic genealogy service.

II. Application

This interim policy applies to: 1) all criminal investigations in which an investigative agency in the Department of Justice ('investigative agency')[3] has exclusive or concurrent jurisdiction of the crime under investigation and the agency has lawful custody, control, or authority to use a forensic sample for FGG/FGGS; or 2) any criminal investigation in which the Department provides funding to a federal, state, local, or tribal agency to conduct FGG/FGGS; or 3) any criminal investigation in which Department employees or contractors conduct genealogical research on leads generated through the use of FGGS; or 4) any federal agency or any unit of state, local, or tribal government that receives grant award funding from the Department that is used to conduct FGG/FGGS.[4]

III. Background

a. STR DNA Typing and CODIS

Forensic DNA typing has historically been used to compare 13-20 STR DNA markers[5] between a forensic sample[6] and one or more reference samples.[7] When a suspect's identity is unknown, a participating crime laboratory may upload a forensic profile[8] into the FBI's Combined DNA Index System (CODIS). CODIS is a law enforcement database that compares DNA profiles derived from forensic samples to those of known offenders.

CODIS was created by the DNA Identification Act of 1994, Pub. L. No. 103-322 (1994), codified at 34 U.S.C. § 12592. This legislation authorized the FBI to create and maintain a national database comprised of designated DNA indices that are routinely searched against one another. If a CODIS search results in a confirmed match between a forensic profile and a known offender, a law enforcement lead is generated and the name of the matching offender is released. If the search does not result in a confirmed match, no lead is generated.

---

[3] As used in this interim policy, the term 'investigative agency' includes any federal, state, local, or tribal law enforcement agency that receives funding from the Department of Justice to conduct FGG/FGGS.

[4] The Department will implement this policy under its federal grant programs (as applicable) through the inclusion of a specific condition(s) in federal awards.

[5] STR DNA typing is a widely-used forensic DNA technology that examines 13-20 (or more) genetic locations on the non-sex chromosomes that contain 2 to 6 base-paired segments known as nucleotides, which tandemly repeat at each location. A 'marker' is a genetic locus, or location.

[6] A 'forensic sample' is biological material reasonably believed by investigators to have been deposited by a putative perpetrator and that was collected from a crime scene, a person, an item, or a location connected to the criminal event. For purposes of this interim policy, the term 'forensic sample' also includes the unidentified human remains of a suspected homicide victim.

[7] A 'reference sample' is biological material from a known source.

[8] As used in this interim policy, 'forensic profile' means an STR DNA typing result, and an STR and/or mitochondrial DNA typing result for unidentified human remains, derived from a forensic sample.

b. Forensic Genetic Genealogical DNA Analysis and Searching

Forensic genealogy is law enforcement's use of DNA analysis combined with traditional genealogy research to generate investigative leads for unsolved violent crimes. Forensic genetic genealogical DNA analysis ('FGG') differs from STR DNA typing in both the type of technology employed and the nature of the databases utilized.

FGG examines more than half a million single nucleotide polymorphisms[9] ('SNPs'), which replace the STR DNA markers analyzed in traditional forensic DNA typing. These SNPs span the entirety of the human genome. This allows scientists to identify shared blocks of DNA between a forensic sample and the sample donor's potential relatives. Recombination or reshuffling of the genome is expected as DNA from each generation is passed down, resulting in larger shared blocks of identical DNA between closer relatives and shorter blocks between more distant relatives. Due to predicted levels of recombination between generations, it is possible to analyze these blocks of genetic information and make inferences regarding potential familial relationships.

Department laboratories currently do not analyze SNPs during forensic DNA casework. Thus, in appropriate cases, it is necessary to outsource biological material to vendor laboratories that perform FGG.[10] After a forensic or reference sample is genotyped by a vendor laboratory, the resulting FGG profile[11] is entered into one or more publicly-available open-data personal genomics DNA databases or direct-to-consumer genetic genealogy services ('DTC service(s)')[12] (collectively referred to herein as 'GG service(s)'). The FGG profile is then compared by automation against the genetic profiles of individuals who have voluntarily submitted their biological samples or entered their genetic profiles into these GG services ('service users'). A computer algorithm is used to evaluate potential familial relationships between the (forensic or reference) sample donor and service users.

It is important to note that personal genetic information is not transferred, retrieved, downloaded, or retained by GG service users — including law enforcement — during the automated search and comparison process. In addition, the investigative use of FGGS involves different DNA technologies, genetic markers, algorithms, and databases from those used by

[9] 'Single nucleotide polymorphisms' are DNA sequence variations that occur when a single nucleotide (A, T, G, or C) in a genomic sequence is altered. These variations may be used to distinguish people for purposes of biological relationship testing.

[10] Contracts with vendor laboratories for FGG services should be reviewed by legal counsel to ensure that they contain appropriate language requiring maintenance of privacy and security controls for handling biological samples, FGG profiles, and other information and data both submitted to, and generated by, those vendor laboratories.

[11] The term 'FGG profile' means the SNP-based genetic profile generated from a forensic or reference sample by a vendor laboratory for the purpose of conducting FGGS.

[12] Direct-to-consumer genetic genealogy services are companies that offer a variety of DNA genomics tests and/or genetic genealogy services directly to the public (rather than through clinical health care providers), typically via customer access to secure online websites.

CODIS. Information and data derived from FGGS is not, and cannot be, uploaded, searched, or retained in any CODIS DNA Index.

IV. Limitations

If the search of an FGG profile results in one or more genetic associations,[13] the GG service typically generates and provides the service user with a list of genetically associated service usernames along with an estimated relationship and (in some cases) the amount of DNA shared by those individuals. A genetic association means that the donor of the (forensic or reference) sample may be related to a service user. However, information derived from genetic associations is used by law enforcement only as an investigative lead. Traditional genealogy research and other investigative work is needed to determine the true nature of any genetic association.

A suspect shall not be arrested based solely on a genetic association generated by a GG service. If a suspect is identified after a genetic association has occurred, STR DNA typing must be performed, and the suspect's STR DNA profile must be directly compared to the forensic profile previously uploaded to CODIS.[14] This comparison is necessary to confirm that the forensic sample could have originated from the suspect.

V. Case Criteria

Investigative agencies may initiate the process of considering the use of FGGS when a case involves an unsolved violent crime[15] and the candidate forensic sample[16] is from a putative perpetrator,[17] or when a case involves what is reasonably believed by investigators to be the unidentified remains of a suspected homicide victim ('unidentified human remains'). In addition, the prosecutor, as defined in footnote twenty of this interim policy, may authorize the investigative use of FGGS for violent crimes or attempts to commit violent crimes other than homicide or sexual offenses (while observing and complying with all requirements of this

[13] A 'genetic association' is determined by the amount of DNA shared between two individuals whose genetic profiles (including, in some cases, an FGG profile) have been entered into a GG service. This amount is measured and reported in centiMorgans. In general, the more DNA shared between two individuals, the higher the number of centiMorgans and the closer the genetic kinship relationship.

[14] Manual comparison is sufficient.

[15] As used in this interim policy, the term 'violent crime' means any homicide or sex crime, including a homicide investigation during which FGGS is used in an attempt to identify the remains of a suspected homicide victim. It also includes other serious crimes and criminal offenses designated by a GG service for which investigative use of its service by law enforcement has been authorized by that service.

[16] A 'candidate forensic sample' is: 1) the remaining portion of a forensic sample or extract being considered for FGGS, and from which a forensic profile was previously derived and uploaded to CODIS; or 2) one or more additional forensic samples or extracts from the same case that share the same forensic profile(s) as that derived from the forensic sample(s) uploaded to CODIS.

[17] A 'putative perpetrator' is one or more criminal actors reasonably believed by investigators to be the source of, or a contributor to, a forensic sample deposited during, or incident to, the commission of a crime.

interim policy) when the circumstances surrounding the criminal act(s) present a substantial and ongoing threat to public safety or national security. Before an investigative agency may attempt to use FGGS, the forensic profile derived from the candidate forensic sample must have been uploaded to CODIS, and subsequent CODIS searches must have failed to produce a probative and confirmed DNA match.

The investigative agency with jurisdiction of either the crime or the location where the unidentified human remains were discovered (if different) must have pursued reasonable investigative leads[18] to solve the case or to identify the unidentified human remains. Finally, when applicable, relevant case information must have been entered into the National Missing and Unidentified Persons System ('NamUs') and the Violent Criminal Apprehension Program ('ViCAP') national database.[19]

VI. Investigative Collaboration

If each of the criteria set forth in Section V has been satisfied, the investigative agency shall contact a designated official at the CODIS laboratory ('designated laboratory official' or 'DLO') that uploaded the forensic profile to CODIS. The DLO must determine if the candidate forensic sample is from a single source contributor or is a deduced mixture. The DLO will also assess the candidate forensic sample's suitability (e.g., quantity, quality, degradation, mixture status, etc.) for FGG and advise the investigative agency about the results of that evaluation. In addition, the DLO may advise the investigative agency of any reasonable scientific alternatives to FGGS, given the nature and condition of the candidate forensic sample, and the availability of other DNA technologies or techniques. The investigative agency shall document its consultation with the DLO.

After consulting with the DLO, the investigative agency shall contact the prosecutor.[20] The investigative agency shall advise the prosecutor of the nature and status of the investigation, the results of the DLO's evaluation of the candidate forensic sample, and any reasonable scientific alternatives to FGGS provided by the DLO.[21] After discussing these issues, and based on the information provided, the prosecutor and the investigative agency must agree that the

[18] 'Reasonable investigative leads' are credible, case-specific facts, information, or circumstances that would lead a reasonably cautious investigator to believe that their pursuit would have a fair probability of identifying a suspect.
[19] This latter requirement only applies if the case meets relevant ViCAP case entry criteria.
[20] As used in this interim policy, the term 'prosecutor' refers, as applicable, to the Assistant Attorney General, United States Attorney, state or local prosecuting attorney, or state attorney general (or his or her designee), with jurisdiction of either the crime under investigation or the location where the unidentified human remains were discovered (if different). When the Department of Justice and one or more state or local prosecuting authorities have concurrent jurisdiction of the crime(s) under investigation, the 'prosecutor' means the Assistant Attorney General, United States Attorney, or the state or local prosecuting official whose office will prosecute the case in the event that charges are filed.
[21] If circumstances permit, it is best practice to have the DLO join (telephonically or otherwise) this meeting. The DLO's participation can help ensure provision of the most complete and detailed information possible regarding sample status, testing options, and possible alternatives to FGGS. This information can, in turn, help optimize subsequent investigative decisions.

candidate forensic sample is suitable for FGG, and that FGGS is a necessary and appropriate step at that stage of the investigation to develop investigative leads or to identify the unidentified human remains. If agreement is reached on these points, FGGS may proceed.

VII. Investigative Caution

Investigative agencies shall identify themselves as law enforcement to GG services and enter and search FGG profiles only in those GG services that provide explicit notice to their service users and the public that law enforcement may use their service sites[22] to investigate crimes or to identify unidentified human remains. The investigative agency shall, if possible, configure service site user settings that control access to FGG profile data and associated account information in a manner that will prevent it from being viewed by other service users.

In certain cases, the genetic association of an FGG profile with a GG service user, in conjunction with subsequent genealogy research, may identify one or more third parties[23] who may have a closer kinship relationship to the donor of the forensic sample than the associated GG service user. In such cases, the acquisition of reference samples from these third parties for the purpose of conducting FGGS may help the investigative agency identify the donor of the forensic sample.

An investigative agency must seek informed consent from third parties before collecting reference samples that will be used for FGGS, unless it concludes that case-specific circumstances provide reasonable grounds to believe that this request would compromise the integrity of the investigation. If that determination is made, the investigative agency shall consult with, and receive approval from, the prosecutor[24] before covertly collecting any reference samples that will be used for FGGS. The investigative agency shall also consult with the DLO, who may provide guidance to investigators about the type and nature of biological samples that may prove most conducive to FGG analysis. Covert collection shall be conducted in a lawful manner. In addition, a search warrant shall be obtained by the investigative agency before a vendor laboratory conducts FGG analysis on any covertly-collected reference sample.

Investigative agencies shall use biological samples and FGG profiles only for law enforcement identification purposes and shall take all reasonable and necessary steps and precautions to ensure that same limited use by others who have authorized access to those samples and profiles. Biological samples and FGG profiles shall not be used by investigative

[22] The term 'service site' means the online web page and content of a GG service.
[23] As used in this interim policy, the term 'third party' means a person who is not a suspect in the investigation.
[24] Before authorization is granted, the prosecutor should notify and consult with the prosecutor in the jurisdiction where the sample will be covertly collected (if different) to ensure that all applicable legal authorities and local procedures relevant to sample acquisition are followed. When the Department of Justice and one or more state or local prosecuting authorities have concurrent jurisdiction of the crime(s) under investigation, the 'prosecutor' means the Assistant Attorney General, United States Attorney, or the state or local prosecuting official whose office will prosecute the case in the event that charges are filed.

agencies, vendor laboratories, GG services, or others to determine the sample donor's genetic predisposition for disease or any other medical condition or psychological trait.

FGGS is a law enforcement technique used to generate investigative leads. Investigative agencies shall not arrest a suspect based solely on a genetic association generated by a GG service. Traditional genealogy research and other investigative work is required to determine the true nature of any genetic association.

VIII. Sample and Data Control and Disposition

All FGG profiles and GG service account information and data shall be treated as confidential government information consistent with any applicable laws, regulations, policies, and procedures. These materials are subject to transfer and disclosure by Department employees and contractors only during the discharge of their official duties and only for authorized purposes.

If a suspect is arrested and charged with a criminal offense while FGG is in progress, the investigative agency shall promptly contact the relevant vendor laboratory or DTC service and direct that all testing cease at a point in time when the (forensic or reference) sample can be preserved. The investigative agency shall also request that the sample, extract,[25] and amplicon[26] be returned directly to the submitting law enforcement agency or custodial CODIS laboratory, as applicable. The investigative agency shall document its request and compliance by the vendor laboratory or DTC service.

If a suspect is arrested and charged with a criminal offense after an FGG profile has been entered into one or more DTC services, the investigative agency shall make a prompt formal request that all FGG profiles and associated account information and data held by any such service be removed from its records and provided directly to the investigative agency.[27] The investigative agency shall document its request and compliance by the DTC service(s). All FGG profiles, account information, and data shall be retained by the investigative agency for potential use during prosecution and subsequent judicial proceedings.

If a suspect is arrested and charged with a criminal offense after an FGG profile has been entered into an open-data personal genomics DNA database, the investigative agency shall promptly remove the FGG profile and all associated account information and data from the database.[28] The investigative agency shall document the removal of this information and data. It

[25] 'Extract' is the total amount of cellular DNA isolated from a biological sample.
[26] 'Amplicon' is the total amount of the targeted DNA segment or sequence generated by the PCR amplification process.
[27] These requests should be made only after the suspect's known STR DNA profile has been manually compared to the forensic profile previously uploaded to CODIS and it has been determined that the profiles match.
[28] The profile, information, and data should be removed only after the suspect's STR DNA profile has been manually compared to the forensic profile previously uploaded to CODIS and it has been determined that the profiles match.

shall be retained by the investigative agency for potential use during prosecution and subsequent judicial proceedings.

Subject to applicable law, in all cases that result in a criminal prosecution, reference samples obtained from third parties for FGGS (including all extracts and amplicon), all derivative FGG profiles, and all GG service account information and data shall be destroyed by the investigative agency only after the entry of an appropriate judicial order. The investigative agency shall document the authorized destruction of these samples, profiles, information, and data.

Subject to applicable government information retention schedules, if FGGS does not result in an arrest and the filing of criminal charges, the investigative agency shall promptly destroy all third-party reference samples (including all extracts and amplicon), all derivative FGG profiles, and all GG service account information and data after their investigative use is complete. The investigative agency shall document the destruction of these samples, profiles, information, and data.

IX. Collection of FGGS Metrics

Each Department component that either uses or funds another agency to use FGG/FGGS for criminal investigative purposes, or that provides any unit of federal, state, local, or tribal government with grant award funding that is used by a grantee to conduct FGG/FGGS for criminal investigative purposes, shall collect and retain the following information on an annual basis: 1) the type of crime investigated; 2) whether FGG/FGGS was conducted on a forensic sample or a reference sample; 3) the type of forensic sample subjected to FGG, and a description of the total amount, condition, and concentration of that sample (e.g., single source, mixed profile, degradation status, etc.); 4) whether FGG analysis resulted in a searchable profile; 5) the identity of the vendor laboratory used to conduct FGG and the GG service(s) used to search the FGG profile; 6) whether the investigation resulted in an arrest that was based, in part, on the use of FGGS; and 7) the total amount of federal funding used to conduct FGG/FGGS in each case.

POLICY FORUM

GENETICS AND PRIVACY

Genealogy databases and the future of criminal investigation

The police can access your online family-tree research—and use it to investigate your relatives

By **Natalie Ram,[1] Christi J. Guerrini,[2] Amy L. McGuire[2]**

The 24 April 2018 arrest of Joseph James DeAngelo as the alleged Golden State Killer, suspected of more than a dozen murders and 50 rapes in California, has raised serious societal questions related to personal privacy. The break in the case came when investigators compared DNA recovered from victims and crime scenes to other DNA profiles searchable in a free genealogical database called GEDmatch. This presents a different situation from the analysis of DNA of individuals arrested or convicted of certain crimes, which has been collected in the U.S. National DNA Index System (NDIS) for forensic purposes since 1989. The search of a nonforensic database for law enforcement purposes has caught public attention, with many wondering how common such searches are, whether they are legal, and what consumers can do to protect themselves and their families from prying police eyes. Investigators are already rushing to make similar searches of GEDmatch in other cases, making ethical and legal inquiry into such use urgent.

In the United States, every state, as well as the federal government, has enacted laws enumerating which convicted or arrested persons are subject to compulsory DNA sampling and inclusion in the NDIS database. The NDIS contains more than 12 million profiles, and it is regularly used to match DNA from crime scenes to identify potential suspects. It is only helpful, however, if the suspect—or a family member of the suspect—has been arrested or committed a crime and their DNA has been collected and stored.

The case of the Golden State Killer is not the first instance of investigators turning to nonforensic DNA databases to generate leads. This was not even the first time investigators used genealogical DNA matches to develop and pursue a suspect in the Golden State Killer case itself. A year before investigators zeroed in on DeAngelo, they subpoenaed another genetic testing company for the name and payment information of one of its users and obtained a warrant for the man's DNA. He was not a match. Similarly, in 2014, Michael Usry found himself the target of a police investigation stemming from a partial genetic match between his father's DNA, stored in an Ancestry.com database, and DNA left at a 1996 murder scene. On the basis of the partial match, police were able to obtain a court order requiring Ancestry.com to disclose the identity of the database DNA match. After mapping out several generations of Usry's father's family, investigators zeroed in on Usry, eventually securing a warrant for his DNA. Ultimately, Usry was cleared as a suspect when his DNA proved not to match the crime scene DNA.

But there have also been reported successes. In 2015, for example, Arizona police arrested and charged Bryan Patrick Miller in the Canal Killer murders based in part on a tip drawn from a genealogical database search (*1*). Searches like these, drawing on genetic information unrelated to the criminal justice system, may offer substantial benefits. Allowing police to conduct similar database searches in other cases is likely to lead to more solved crimes. Moreover, expanding law enforcement investigations to encompass genealogical databases may help to remedy the racial and ethnic disparities that plague traditional forensic searches. In accordance with state laws, official forensic databases are typically limited to individuals arrested or convicted of certain crimes. Racial and ethnic disparities throughout the criminal justice system are therefore reproduced in the racial and ethnic makeup of these forensic databases. Genealogical databases, by contrast, are biased toward different demographics. The 23andMe database, for instance, consists disproportionately of individuals of European descent. Including genealogical databases in forensic searches might thus begin to redress, in at least one respect, disparities in the criminal justice system.

There are few legal roadblocks to police use of genetic databases intended to help individuals explore their health or identify genetic relatives. The Fourth Amendment's protection against warrantless searches and seizures generally does not apply to material or data voluntarily shared with a third party, like a direct-to-consumer genetics testing or interpretation company or a genetic matching platform like GEDmatch. Once an individual has voluntarily shared her data with a third party, she typically cannot claim any expectation of privacy in those data—and so the government need not secure a warrant before searching it.

Beyond the Constitution, three federal laws protect some genetic data against certain disclosures, but these too are unlikely to provide an effective shield against law enforcement searches in nonforensic genetic databases. The Genetic Information Nondiscrimination Act (GINA) protects genetic data, but only against certain uses by employers and health insurers (*2*). GINA provides no protection against law enforcement searches. Similarly, most companies and websites offering DNA testing, interpretation, or matching services directly to individuals likely are not covered by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, which governs the use and disclosure of identifiable health information. These providers are usually careful to explain that they are not engaged in health care or the manipulation or provision of health data (*3*). Finally, although certificates of confidentiality protect scientific researchers from disclosing data to law enforcement—even against a warrant (*4*)—they do not extend to scenarios in which law enforcement is just another contributor to and user of online genetic resources, such as public databases and matching tools. Certificates of confidentiality have faced few challenges in court, and so it is also uncertain whether the protection they purport to provide will hold up against a challenge by law enforcement seeking access.

Consistent with this legal landscape, companies and websites that generate, interpret, or match genetic data directly for individuals often do not promise complete protection. In terms of law enforcement, for instance, 23andMe states in its privacy policy, "23andMe will preserve and disclose any and all information to law enforcement agencies or others if required to do so by law or in the good faith belief that such preservation or disclosure is reasonably necessary to…comply with legal or regulatory process (such as a judicial proceeding, court order, or government inquiry)…" (*5*). Ancestry.com similarly

[1]University of Baltimore School of Law, Baltimore, MD, USA. [2]Center for Medical Ethics and Health Policy, Baylor College of Medicine, Houston, TX, USA. Email: nram@ubalt.edu; amcguire@bcm.edu

discloses, "We may share your Personal Information if we believe it is reasonably necessary to: [c]omply with valid legal process (e.g., subpoenas, warrants)..." (*6*). And in the wake of the Golden State Killer arrest, GEDmatch has altered its terms of service to explicitly permit law enforcement use of its database to investigate homicides and sexual assault (*7*). Although these disclaimers are usually unambiguous, they are sometimes buried in terms of service or privacy policies that many individuals do not take care to read or fully understand.

Despite the lack of legal protection against law enforcement searches of nonforensic databases, such searches may run counter to core values of American law. The Fourth Amendment is a constitutional commitment to protect fundamental civil rights. Part of that is a commitment to protecting privacy or freedom from government surveillance. Police cannot search a house without suspecting a specific individual of particular acts—even if doing so would enable the police to solve many more crimes. Yet, database searches permit law enforcement to search the genetic data of each database member without any suspicion that a particular member is tied to a particular crime. Although the U.S. Supreme Court has approved suspicionless genetic searches for individuals with diminished expectations of privacy, like those arrested or convicted of crimes (*8*), ordinary members of the public are different. Familial searches, like those used in the Golden State Killer investigation, are an even further departure from the Supreme Court standard. Certainly, individuals who commit crimes and leave their DNA behind forfeit any expectation of privacy in that DNA. But a usable forensic identification requires two matching parts: a crime scene sample and a database profile that matches it. Suspects identified through familial searches cannot be said to have voluntarily shared their genetic profile in a database of known individuals, even if a genetic relative has.

The Supreme Court is poised to reconsider its broad rule that the voluntary sharing of data negates expectations of privacy—and thus negates Fourth Amendment protections against warrantless government searches. In *Carpenter* v. *United States*, the Supreme Court will determine whether police must obtain a warrant to justify access to historical cell phone records revealing the movements and location of a cell phone user over a long period of time (*9*). In the digital age, in which nearly all data are at least nominally shared with third parties like internet service providers, website hosts, and cell phone companies, the current rule means that the Fourth Amendment often does not apply. *Carpenter* may reshape this rule to account for the realities of a big-data world. A ruling in *Carpenter* that limits police use of historical cell phone data may substantially affect police practices surrounding genetic data as well, as merely sharing data with another might well be insufficient to permit its suspicionless search by the government for crime-detection purposes.

Even if the Supreme Court decision in *Carpenter* does not revamp Fourth Amendment rules governing police access to shared data, the setting of that case suggests another way to resolve concerns about police access to nonforensic genetic databases. In the Stored Communications Act, Congress provided substantial statutory protection for email and other digital information maintained on the internet. Under the act, a court may order disclosure of electronic records if the government "offers specific and articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation" (*10*). This standard is less onerous than the Fourth Amendment's warrant requirement, but it is notably more demanding than any protections the law currently provides.

Enacting similar protection for genetic data stored in nonforensic databases would ensure that the government cannot subject ordinary individuals to suspicionless genetic searches, while allowing investigators to access genetic data where there is reason to believe a particular individual may be tied to a particular crime. A Stored Genetics Act would likely render law enforcement searches of nonforensic genetic databases unlawful for crime-detection purposes, as there can be no "specific and articulable" connection between particular database records and a particular crime when investigators seek to use such a search to generate leads, not investigate them. Thus, although such an approach would preserve freedom from perpetual genetic surveillance by the government, it may well result in fewer solved cases.

Legislatures may understandably be loath to enact a total prohibition of such searches. At a minimum, however, policy-makers should delineate under what circumstances such searches are acceptable. For example, several states, including California, Colorado, and Texas, have identified prerequisites to the use of familial searches of the state's own forensic database, including that the crime to be investigated is serious and that traditional investigative techniques have been exhausted without success (*11*). Similar constraints could be placed on law enforcement searches of nonforensic databases. The challenge of this approach is that limitations on the scope of use can erode quickly. Thus, although Colorado's policy governing familial searches of the state's forensic database limits such searches to crimes with "significant public safety concerns," police in that state used a familial search to solve a car break-in where the perpetrator "left a drop of blood on a passenger seat when he broke a car window and stole $1.40 in change" (*11*). The erosion of limits on crime-solving technology may well be inevitable, and it threatens our collective civil liberties and opens the door to socially and politically unacceptable genetic surveillance.

Whatever legislative solution is adopted, it must at least take into account public perspectives to clearly delineate acceptable uses and balance the social benefit of solving cases with individuals' interests in avoiding unwarranted government scrutiny. ■

ILLUSTRATION: LUSH/123RF

REFERENCES AND NOTES

1. M. Cassidy, "How forensic genealogy led to an arrest in the Phoenix 'Canal Killer' case," Arizona Republic, 10 November 2016; www.azcentral.com/story/news/local/phoenix/2016/11/30/how-forensic-genealogy-led-arrest-phoenix-canal-killer-case-bryan-patrick-miller-dna/94565410/.
2. 122 Statute 881.
3. J. Hsu, *I/S: A Journal of Law & Policy for the Information Society (Moritz College of Law)* **6**, 557 (2011).
4. 42 United States Code (U.S.C.) § 241 (d).
5. www.23andme.com/about/privacy/.
6. www.ancestry.com/cs/legal/privacystatement.
7. https://bit.ly/2IZKzGt.
8. *Maryland* v. *King*, 133 S. Ct. 1958 (2013).
9. *Carpenter* v. *United States*, No. 16-402 (argued 29 November 2017).
10. 18 U.S.C. § 2703 (d).
11. N. Ram, *Stanford Law Rev.* **63**, 751 (2011).

ACKNOWLEDGMENTS

Funding was provided by the National Institutes of Health, National Human Genome Research Institute (K01 HG009355 and R01 HG008918). We thank M. Majumder, D. Peterson, S. Pereira, R. Hsu, A. Gutierrez, and J. Robinson for contributions and assistance on this project.

10.1126/science.aau1083

Genealogy databases and the future of criminal investigation

Natalie Ram, Christi J. Guerrini and Amy L. McGuire

Science **360** (6393), 1078-1079.
DOI: 10.1126/science.aau1083