THE GEORGE WASHINGTON UNIVERSITY

WASHINGTON, DC

SONIA M. SUTER
THE KAHAN FAMILY
RESEARCH PROFESSOR OF LAW
TELEPHONE :(202) 994-9257
FAX: (202) 994-5614

Law School

Testimony of Sonia M. Suter, JD, MS,
The Kahan Family Research Professor of Law
Founding Director, Health Law Initiative
The George Washington University Law School
Before the Maryland Senate Judicial Proceedings Committee
March 10, 2020

Thank you, Chair Smith, Vice Chair Waldstreicher, and honorable members of the Senate Judicial Proceedings Committee for your consideration of SB 848. I am a law professor at The George Washington University Law School, where I teach courses that address bioethics and issues at the intersection of law, medicine, and science. As a former genetics counselor, I have carved out an area of expertise in law and genetics, including co-authoring the forthcoming textbook, GENETICS: ETHICS, LAW AND POLICY (5th ed. 2020).

I want to begin by first commending this Committee for being at the forefront in considering legislation to regulate the emerging technology of forensic genetic genealogy (FGG). FGG is unquestionably a powerful forensic tool with the potential to solve cold cases, to exonerate the innocent, and honor victims' interests in seeing justice done. Even so, as I noted in my testimony to the House Judiciary Committee in the Hearings on Familial DNA and Criminal Investigations in November, 2019, this technology raises serious privacy and civil liberty concerns. I applaud the efforts of Senator Sydnor and Delegate Shetty in shepherding legislation that strives to balance the potential benefits of FGG against its potential threats. I respectfully submit this testimony to support many aspects of the proposed bill and to encourage some friendly amendments, which I believe are within the spirit of this proposed legislation.

The Privacy and Civil Liberty Concerns of FGG

Before highlighting the strengths of the bill and offering friendly amendments, I want to briefly lay out the specific privacy/civil liberty risks that this technology presents.

1. The FGG genetic profiles (SNP profiles) contain a wealth of information

The "DNA fingerprints" used in the CODIS and SDIS DNA databases are based on STR profiles,[1] which are intended to provide only identifying information. For all intents and

[1] These profiles are based on analysis of repeated sequences (short-tandem repeats) at 13-20 locations within the genome.

purposes, STRs reveal very little, if anything, about someone's health information. In contrast, the SNP profiles used in FGG, which are based on analysis of hundreds of thousands of variations in the genome called single-nucleotide polymorphisms, generate much more information than STR profiles.[2] Not only can SNPs locate biological relatives and provide information about ancestry, they can also identify predisposition to certain diseases (like heritable forms of breast cancer or Alzheimer's disease) or traits (such as whether someone sneezes in bright light).[3] As a result, it would not take much effort to determine an individual's disease risks based solely on SNP profiles. Courts have repeatedly emphasized that STR profiles are no more threatening to privacy interests than ordinary fingerprints because they only provide identifying information.[4] The same cannot be said for the SNP profiles used in FGG. As a result, FGG raises significant privacy concerns because of the potential for law enforcement (via vendor laboratories) to access such widely informative profiles.

2. FGG raises (familial) privacy concerns

Like traditional familial searches, which Maryland bans, FGG raises the possibility of uncovering secrets regarding adoption, egg or sperm donation, paternity, and maternity, which can disrupt the integrity of the family. It also subjects putative biological relatives of the source of crime scene samples to government surveillance simply because of presumed genetic relatedness (i.e., sharing a certain percentage of DNA). However, whereas STR profiles typically only extend to first-degree relatives, who are more likely to be known to the source of the profile as parents, siblings, or children,[5] SNPs can link individuals to third, fourth, or even ninth or more distant cousins.[6] As a result, a familial search of direct-to-consumer (DTC) databases can cast a very wide net, including not only known and close relatives, but also distant and unknown relatives, thereby increasing the odds of uncovering family secrets.

FGG also involves more than assessing the percentage of shared DNA between two individuals. To establish the biological relationship with someone who shares a certain percentage of DNA – for example, to determine if the other person is an aunt/uncle, grandparent, grandchild, half sibling, or nephew/niece – family trees must be constructed using public and other records, such as birth certificates, obituaries, adoption records, and social-media profiles.[7] This additional level of governmental investigation into biological and social connections,

---

[2] Erin Murphy, *Law and Policy Oversight of Familial Searches in Recreational Genealogy Databases*, 292 FORENSIC SCI. Int'l e5, e5 (2018). The DOJ Interim policy notes that such searches involve "more than a million" SNPs. Interim Policy, *supra* note 9, at 3.

[3] MAXWELL J. MEHLMAN, MARK A. ROTHSTEIN, & SONIA M. SUTER, GENETICS: ETHICS, LAW AND POLICY 382 (6th ed. 2020 forthcoming).

[4] Maryland v. King, 569 U.S. 435, 459 (2013).

[5] Murphy, *supra* note 2, at e6.

[6] United States Department of Justice Interim Policy Forensic Genetic Genealogical DNA Analysis and Searching, at 4, https://www.justice.gov/olp/page/file/1204386/download [hereinafter Interim Policy]

[7] Sarah Zhang, *The Messy Consequences of the Golden State Killer*, ATLANTIC, Oct. 1, 2019, https://www.theatlantic.com/science/archive/2019/10/genetic-genealogy-dna-database-criminal-investigations/599005/.

amplifies the potential intrusion into personal and familial privacy. While one might argue that people enter their DNA profiles into DTC databases precisely because they want to discover unknown relatives, it is one thing to discover this for yourself and quite another to have law enforcement prying into the contours of one's social and biological family trees.

Moreover, because familial searches in consumer databases are "long-range familial searches,"[8] they subject potentially hundreds of people to examination of their more sensitive SNP profiles and familial connections. The potential of FGG to cast such a wide net multiplies the privacy concerns described above.

3. The source of profiles in DTC databases do not have reduced privacy interests

Courts have found that the mandatory collection of DNA from convicted offenders and certain arrestees to create STR profiles for CODIS/SDIS databases does not violate the Fourth Amendment. One rationale is that convicted offenders have reduced expectations of privacy;[9] another is that STR profiles do not reveal sensitive information.[10] Those rationales do not apply to the individuals who share their DNA with DTC DNA services to learn about ancestry, disease information, and/or traits. Their use of these services should not automatically forfeit their ability to control the use of their SNP profiles for other purposes. This principle is especially important because, as noted above, unlike STRs, SNPs hold a wealth of potentially sensitive information. Therefore government access to these databases, either directly or through the use of vendor labs, raises serious privacy concerns.

4. FGG involves the use of unregulated vendor labs

Because law enforcement laboratories do not have the expertise or legal authority to create the SNP profiles necessary for FGG, they must outsource the genotyping of crime scene and reference samples to private companies.[11] This means that two actors – the government and a vendor laboratory – potentially have access to the SNP profiles, heightening the privacy concerns. Whereas law enforcement forensic labs must comply with a series of requirements, including accreditation and the hiring of qualified personnel,[12] such regulations do not apply to the vendor laboratories used for FGG. In fact, these labs are largely unregulated.

---

8 Yaniv Erlich et al., *Identity Inference of Genomic Data Using Long-Range Familial Searches*, 362 SCI. 690 (2019).

9 Sonia M. Suter, All in the Family: Privacy and DNA Familial Searching, 23 HARV. J. L. & TECH. 309, 329-30 (2010).

10 Maryland v. King, 569 U.S. 435 (2013).

11 Interim Policy, *supra* note 6, at 3.

12 https://www.fbi.gov/services/laboratory/biometric-analysis/codis#NDIS-Operational%20Procedures%20Manual.

5. The lack of regulation of direct-to-consumer (DTC) databases

Whereas statutes and regulations govern whose profiles can be included in the CODIS and SDIS databases, the nature of the DNA profiles that are used, and how the databases can be searched, virtually no regulation governs the use of DTC DNA databases,[13] let alone their use by law enforcement. The Interim Policy issued by the Department of Justice (DOJ) in Nov. 2019 "is the first substantial attempt to address 'how genetic genealogy should be done.'"[14] Its reach, however, is limited, and it does not apply to typical, local law enforcement uses of FGG.[15]

Balancing the Benefits and Risks of FGG

Many of the concerns that FGG raises are similar to, or in some ways more significant than, the concerns of familial searches, which Maryland already bans. The power of FGG to solve crimes, however, is greater than that of traditional familial searches (which only extend to first-degree relatives). In addition, FGG is also emotionally compelling because it provides tangible and easily measured benefits: improving public safety by identifying and imprisoning violent perpetrators, vindicating victims' interests, and exonerating the innocent. In contrast, the risks associated with FGG concern amorphous interests like privacy and civil liberties. When set against the potential to imprison a serial murderer or rapist, these other interests often seem insufficiently weighty or concrete.

To try to balance these conflicting interests, policy makers should recognize they have prima facie duties with respect to both competing goals – to solve crimes and to prevent threats to privacy and civil liberties. Even if the value of FGG outweighs its risks, "the overridden values do not go away; they retain 'moral traces.'" These "moral traces" compel regulation of the technology to minimize its threats to those values and maximize the benefits it offers.[16]

SB 848 is well on its way to achieving the necessary regulation of FGG. Nevertheless, there are several areas where the proposed legislation could go do more to ensure that FGG is used in a manner that protects some of the overridden values. Drawing heavily on, but also supplementing, the DOJ Interim Policy, I describe below 1) the areas where SB 848 is successful in addressing the overridden values and 2) the areas where these efforts could be bolstered.

---

13 James W. Hazel Y Christopher Slobogin, *Who Know What and When?: A Survey of the Privacy Policies Preferred by U.S. Direct-to-Consumer Genetic Testing Companies,* 28 CORNELL J. L. & PUB. POL'Y 35 (2018)

14 Thomas F. Callaghan, *Responsible Genetic Genealogy*, 366 SCI. 155 (2019).

15 Interim Policy, *supra* note 6 at 2 (describing that the policy only applies to criminal investigations under the DOJ's jurisdiction or funded by the DOJ or to research on this technology involving DOJ employees or contractors or performed by federal agencies or governmental units with DOJ grants).

16 Suter, *supra* note 9, at 372-79.

Where SB 848 Is Successful in Balancing the Respective Interests
(with suggestions for friendly amendments)

1. Limit FGG searches of DTC databases to the profiles and/or samples of sources who have consented to such searches by law enforcement

Section 2-506(E) of SB 848 achieves this goal. Although it may reduce the number of potential links to perpetrators of unsolved crimes, this provision ensures that people do not become genetic informants or subject to government surveillance simply by virtue of sharing a certain percentage of DNA with perpetrators of unsolved crimes. Moreover, SB 848 limits law enforcement access to DTC profiles based on individuals' *express* willingness to participate, rather than relying on whether DTC services provide notice that law enforcement may use their services, as suggested by DOJ's Interim Policy.[17] Consumers can easily overlook such notices because they are buried in the terms of agreements of DTC. Moreover, relying only on notices, as opposed to affirmative consent, does not protect the agency of the consumers. As a result, section 2-506(E) provides an important privacy protection.

2. Limit the reach of FGG to more closely related relatives

Section 2-506(G) achieves this protection by limiting genetic genealogy investigations to searches that generate a "match within a third degree of relatedness." In other words it doesn't allow searches that go beyond great grandparents, great grandchildren, great uncles/aunts, and first cousins. Although the DOJ Interim Policy does not include such a provision, I believe this protection is an important way to balance the privacy concerns and law enforcement interests in FGG. It limits the size of the net cast by FGG, thereby minimizing the number of biological relatives of the perpetrator who might be subject to government surveillance. Moreover, it decreases the chances of discoveries of family secrets related to adoption, adultery, gamete donation, etc. To be sure this provision draws a line that may, in some cases, preclude potentially helpful uses of FGG. The goal of SB 848, however, is to offer a compromise between banning FGG and allowing its unlimited use.

3. Regulations should require *informed consent* to collect references samples from third parties

When an investigation requires samples from third parties (who are not suspects) to assist in or expedite the construction of a family tree, regulations should clearly prohibit surreptitious collection of samples from these individuals. Instead, *informed consent* should be required for police to obtain and analyze biological samples from them. Such requirements ensure that individuals are not subject to government surveillance merely because of their potential genetic relatedness to the perpetrator of the crime.

Section 2-504(A) captures the spirit of this recommendation by prohibiting the collection of DNA samples from "an individual without the knowledge and consent of the individual who is to

[17] Interim Policy, *supra* note 6, at 6.

provide the DNA sample."[18] It does not, however, require that the consent be *informed*, which is necessary to prevent people from granting consent based on deception or misrepresentation.[19] Ideally, SB 848 would not only *require* that consent be informed, but would also include provisions to ensure that consent is *truly* informed. For example, it could require individuals with expertise in genetic counseling, genetic genealogy, and other relevant disciplines to shape the informed consent process. Thus, a friendly amendment would mandate *informed* consent for the collection of DNA from third parties who are not suspects in the investigation, with provisions to ensure that the process of obtaining informed consent is as effective as possible.

The DOJ Interim Rule includes an exception in cases where there is "reasonable belief" that informed consent would compromise the investigation. It also requires a search warrant to create a SNP profile on "any covertly-collected" samples from such third parties.[20] Section 2-506(F) of SB 848 explicitly precludes such an exception by prohibiting the issuance of "a warrant, subpoena, or court order . . . to compel access to an individual's DNA record, DNA sample, or other DNA related data from a direct-to-consumer genetic genealogy service if the individual does not consent to the search by a law enforcement agency." There may be a case for some narrow exceptions to the consent requirement. If any such exceptions are added, however, they must require judicial supervision and oversight, which the Interim Rule does not mandate. Without such oversight, the exception could easily swallow the rule.

4. Provide transparency regarding FGG

Section 2-506 (H) requires full reporting of the FGG investigation, including "any findings in source categories of nongenetic investigatory material . . . to the investigating law enforcement agency." This provision is a first step in promoting public trust and transparency. Those goals would be further advanced, however, by requiring annual disclosure to the *defense* and to the *public* about the nature of genetic testing for FGG, the types of nongenetic sources used to construct the family trees, how many samples were collected in the investigations, and the outcomes of the investigations.

Where SB 848 Could Do More to Balance the Respective Interests

1. Limit the use of FGG to serious and violent crimes

The DOJ Interim Policy limits the use of FGG to investigations of "unsolved violent crimes," defined as "any homicide or sex crime," or to identify "the remains of a suspected homicide

[18] This provision raises an issue of whether there should be a blanket prohibition of surreptitious collection of DNA from everyone in all instances, including when the government has probable cause to believe an individual has committed a crime.

[19] Jon Schuppe, *Police Told a Mother Her DNA Would Identify a Dead Relative. They Arrested Her Son Instead,* NBC News, Feb. 22, 2020

[20] Interim Policy, *supra* note 6, at 6.

victim."[21] It creates an exception for the investigation of "violent crimes other than homicide or sexual offenses," if the circumstances suggest "the criminal act(s) present a substantial and ongoing threat to public safety or national security."[22] The privacy and liberty threats of FGG can only be justified by trying to achieve significant goals like identifying serious rapists and murders. Lesser crimes do not warrant such intrusions. Consistent with this view are the results of a recent survey, which found that a strong majority (91%) of participants support the use of this technology to solve violent crimes like rape and murder, while under half (46%) support its use to solve nonviolent crimes.[23] Thus, I respectfully recommend that SB 848 narrow its application to *only* "a crime of violence or an attempt to commit a crime of violence" (2-504(B)(3)(i)(1)), but *not* to "burglary or an attempt to commit burglary" (2-504(B)(3)(i)(2)).[24]

2. Require that SNP profiles be used only for identification purposes

This requirement addresses one of the most significant privacy concerns: the fact that law enforcement (or vendor labs) could use the SNP profiles to discover sensitive information about an individual, such as disease risks or psychological traits. The DOJ Interim Rule imposes such a requirement and prohibits the use of biological samples or genetic profiles to determine "predisposition for disease or any other medical condition or psychological trait." Furthermore, it requires law enforcement to "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."[25] Such provisions are essential to minimize the privacy risks of FGG and to promote public trust. Moreover, they do not limit the effectiveness of FGG at all.

3. Only allow FGG after all reasonable investigative leads have been pursued

Law enforcement may become entranced by the power of FGG to the exclusion of other investigative techniques that can be as or more useful in identifying perpetrators. Ensuring that the most appropriate techniques are used increases successful investigations. Such a requirement would also limit the frequency of the use of FGG, thereby reducing some of the associated risks. The DOJ Interim Policy requires law enforcement to "have pursued reasonable investigative leads to solve the case or identify the unidentified human remains."[26] I respectfully suggest that SB 848 include a similar requirement. Moreover, to ensure that law enforcement complies with such a requirement, it should require judicial oversight to establish that "reasonable investigative leads" have been pursued and that FGG is an appropriate forensic technique under the circumstances. Such a provision would maximize the benefits of FGG while minimizing its risks.

---

21 Interim Policy, *supra* note 6, at 4.

22 *Id.* at 4-5.

23 Christi J. Guerrini et al., *Should Police Have Access to Genetic Genealogy Databases? Capturing the Golden State Killer and Other Criminals Using a Controversial New Forensic Technique*, 16 PLOS BIO. 1 (2018).

24 I should note that the statute is not consistent in that it only refers to "a crime of violence" in 2-506(e)(2)(I), but not also to an *attempt* to commit a crime of violence," (2-504(B)(3)(i)(1).

25 Interim Policy, *supra* note 6, at 6-7.

26 *Id.* at 5.

4. Limit access to and control of profiles and samples used in FGG

The DOJ Interim Policy offers recommendations that largely achieve these goals. For example, it states that once the FGG investigation leads to an arrest and criminal charge, the vendor laboratory or DTC service should discontinue any ongoing genetic analysis and return all genetic profiles and samples used in the investigation to the investigative agency. In addition, if a SNP profile has been entered into a DTC service, law enforcement must request that the DTC service remove all SNP profiles created for the FGG (and associated account information) from its records and provide them "directly to the investigative agency." If the forensic SNP profile has been entered into an open-data personal genomics DNA database, law enforcement "must remove the profile and all associated account information and data from the database."[27]

It is particularly important that biological samples, derivative SNP profiles, and "family tree" information created from third parties (who were never suspects) be destroyed once a criminal prosecution results or the investigation ends. The DOJ Interim Policy makes such destruction contingent on a court order in cases where the investigation leads to a criminal prosecution, but automatic in cases that that do not result in arrest or the filing of charges.[28] I would argue the destruction should be automatic and should not require affirmative requests by third parties in all cases. This requirement minimizes the chance of law enforcement agencies creating unregulated, shadow databases, which threaten privacy interests.

Finally, consistent with the DOJ Interim policy, privacy protections would be strengthened by requiring that all parties who have access to genetic profiles, samples, and information created for purposes of FGG treat such information as "confidential government information."[29] The fact that vendor laboratories are necessary to assist with FGG investigations and involved in the analysis of information-rich SNP profiles requires that there be adequate oversight of these entities, which are largely unregulated.

Conclusion

FGG requires difficult balancing of competing societal goals. Although the power of FGG to solve crimes is great, the risks it poses are sufficiently important to require regulations that minimize its threats to privacy and civil liberty interests. I support Senator Sydnor and Delegate Shetty in their efforts to sponsor legislation that addresses these issues. I believe my proposed friendly amendments will not only strengthen the protections of SB 848, but will also promote public trust, which is essential to maximize the benefits of FGG.

---

27 *Id.*
28 *Id.* at 8.
29 *Id.*