4-2020

Why We Fear Genetic Informants: Using Genetic Genealogy to Catch Serial Killers

Teneille R. Brown

THE COLUMBIA
SCIENCE &
TECHNOLOGY
LAW REVIEW

VOL. XXI STLR.ORG FALL 2019

WHY WE FEAR GENETIC INFORMANTS: USING GENETIC GENEALOGY TO CATCH SERIAL KILLERS

Teneille R. Brown, JD*

This Article proceeds in three parts. In the first part, I explain the rise of genetic genealogical testing and how it is employed by police for forensic genetic genealogy *(FGG). I also clarify how FGG is different from a traditional search of the federal Combined DNA Index System (CODIS) database. In the second part, I challenge the many concerns that scholars have raised in response to FGG. Specifically, I counter the arguments that it violates the Fourth Amendment, invades the privacy of innocent individuals, renders people unintentional genetic informants, improperly relies on police deception and the involuntary participation of suspects, and creates a de facto federal database. These concerns reflect misunderstandings of ordinary criminal procedure, the legal might of online user "agreements," and the distinctions between clinical research and criminal law. In the third part, I provide a unique theory for why we seem to fear "genetic informants." I conclude with a call for more nuanced policy measures that will better protect genetic privacy consistent with consumer expectations, while still permitting the use of FGG to deliver justice to victims and help convict serial killers and rapists.*

* Teneille R. Brown J.D. is a Professor of Law at the University of Utah, S.J Quinney College of Law, and an adjunct Professor in the Department of General Internal Medicine. This research was made possible, in part, through generous support from the Albert and Elaine Borchard Fund for Faculty Excellence and funding from the Utah Center for Excellence in ELSI Research (UCEER). UCEER is supported by the National Human Genome Research Institute of the National Institutes of Health under Award Number P20HG007249. The content is solely the responsibility of the author and does not necessarily represent the official views of the National Institutes of Health.

I. INTRODUCTION

Consumer genetics has exploded, driven by the second-most popular hobby in the United States: genealogy.[1] Kits from the market leaders—23andMe and Ancestry—are top-sellers on Black Friday.[2] As the Centers for Disease Control and Prevention reports, ancestry tests that have been bundled with information on genetic health risks are selling "like hotcakes," and direct-to-consumer (DTC) genetic tests have "continued to skyrocket."[3] These kits allow users to submit a saliva sample through the mail, without the involvement of a physician, and test for about 700,000 genetic mutations. The results are then returned to them online.

This "hobby" has been co-opted by law enforcement to solve cold cases. Officers can link crime-scene DNA with the DNA of one of the assailant's relatives, which had been previously uploaded to a non-forensic, DTC genetic database. A 2018 study predicted that within a couple of years roughly 90% of Americans of European descent will be genetically identifiable in this way, even those who have never submitted a saliva sample nor been tested themselves.[4] A

1. Scott Bowen & Muin J. Khoury, *Consumer Genetic Testing Is Booming: But What Are the Benefits and Harms to Individuals and Populations?*, CENTER FOR DISEASE CONTROL: GENOMICS AND PRECISION HEALTH (June 12, 2018), https://blogs.cdc.gov/genomics/2018/06/12/consumer-genetic-testing.

2. Shanna Mason, *Privacy of Information and DNA Testing Kits*, 27 CATH. U.J.L. & TECH. 161, 161 (2018) ("In 2017, AncestryDNA sold roughly 1.5 million kits from Black Friday through Cyber Monday, triple the amount of sales from 2016.").

3. Bowen & Khoury, *supra* note 1.

4. Yaniv Erlich et al., *Identity Inference of Genomic Data Using Long-Range Familial Searches*, 362 SCIENCE 690, 690 & 691 fig.1 (2018); *see also* Heather Murphy, *Most White Americans' DNA Can Be Identified Through Genealogy Databases*, N.Y. TIMES (Oct. 11, 2018), https://www.nytimes.com/2018/10/11/science/science-genetic-genealogy-study.html?module=inline.

relative's genetic data can act as a silent witness, or genetic informant, against the person who left the DNA at the crime scene. This "genetic informant" wordlessly guides law enforcement to a handful of potential suspects, by simply informing them that the suspect is very likely a third-cousin, nephew, or grandson of the person in the DTC database. Public records and newspaper clippings then provide the necessary details to put a name and location to the crime-scene DNA.

At least thirty murderers and rapists have been arrested after detectives identified them through a combination of genetic testing and genealogy research tools. This general method has been dubbed "genetic genealogy"—the use of DNA to infer relationships between individuals.[5] Given the hundreds of thousands of cold cases in the U.S., with some unknown number of case files containing DNA samples, experts predict that genetic genealogy will become a multimillion dollar forensic business.[6] One method in particular, called "forensic genetic genealogy," or FGG, has allowed law enforcement to significantly reduce the size of the suspect pool when no other good leads exist.[7]

The public generally seems to support the use of genetic genealogy to apprehend violent criminals in cold cases, even when the individual contributing her DNA to a genealogical website had no notice her sample would be used in this way.[8] However, legal scholars have sounded many alarms. In op-eds in the New York

5. Peter Aldous, *The Golden State Killer Case Has Spawned a New Forensic Science Industry*, BUZZFEED NEWS (Feb. 15, 2019), https://www.buzzfeednews.com/article/peteraldhous/genetic-genealogy-dna-business-parabon-bode.

6. *Id.*

7. Ellen Greytak et al., *Privacy and Genetic Genealogy Data*, 361 SCIENCE 857 (2018); *Interim Policy: Forensic Genetic Genealogical DNA Analysis and Searching*, DEP'T OF JUSTICE 6 (2019), www.justice.gov/olp/page/file/1204386/download; Heather Murphy, *Genealogists Turn to Cousins' DNA and Family Trees to Crack Five More Cold Cases*, N.Y. TIMES (June 27, 2018), https://www.nytimes.com/2018/06/27/science/dna-family-trees-cold-cases.html (Referring to FGG as "long range familial searches," or LRFS).

8. The majority of Americans polled support police searches of genetic websites that identify genetic relatives and disclosure of DTC genetic testing customer information, as well as creation of fake profiles of individuals by police on genealogy websites. Respondents were much more supportive of these activities when the purpose was to identify perpetrators of violent crimes than when the purpose was to identify perpetrators of nonviolent crimes. However, the sample was more likely than the rest of the population to have been the victim of a crime. *See* Christi 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 BIOLOGY e2006906, *3 (2018).

Times[9] and Slate,[10] in scientific and legal scholarly articles,[11] and in lobbying efforts with their legislatures,[12] legal scholars have called for limitations or bans on these practices. Some propose requiring law enforcement to get warrants before police can access DTC genetic databases or immediately banning FGG and other genetic genealogy tools. In Maryland, legislators proposed a bill in 2019 to prohibit the searching of genealogical databases to find distant relatives of criminal suspects.[13]

The opponents' concerns are many, but they can generally be boiled down to fears that these new methods will invade the privacy and autonomy of presumptively innocent individuals by creating an involuntary and *de facto* forensic genetic database.[14] These concerns, I argue, are considerably overblown. Indeed, many aspects of FGG implicate nothing new, legally or ethically, and might even *better* protect the privacy of innocent individuals. That's right. This methodology might *reduce* the privacy violations that are rampant in ordinary police investigations. So why are so many legal scholars fascinated by genetic genealogy yet fear a world where law enforcement uses FGG? What is it about this methodology that triggers knee-jerk calls to ban the use of "genetic informants?"

We are right to be concerned about unleashing private, genetic information to the government or private actors. We are still

---

9. Elizabeth Joh, Opinion, *Want to See My Genes? Get a Warrant*, N.Y. TIMES (June 11, 2019), https://www.nytimes.com/2019/06/11/opinion/police-dna-warrant.html.

10. Natalie Ram, *The U.S. May Soon Have a De Facto National DNA Database,* SLATE (Mar. 19, 2019, 7:30 AM), https://slate.com/technology/2019/03/national-dna-database-law-enforcement-genetic-genealogy.html.

11. Natalie Ram et al., *Genealogy Databases and the Future of Criminal Investigation*, 360 SCIENCE 1078, 1079 (2018).

12. Natalie Ram, *Incidental Informants Police Can Use Genealogy Databases to Help Identify Criminal Relatives-but Should They*?, MD. B.J., July-Aug. 2018, at 8, 10.

13. H.B. 30, 440th Gen. Assemb., Reg. Sess., (Md. 2019) ("For the purpose of prohibiting a person from performing a search of a certain DNA or genealogical data base for the purpose of 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; and generally relating to DNA analysis.").

14. Privacy is a multifaceted concept that can include the right to be left alone, to be free from surveillance, to remain anonymous, to keep your information confidential, or entirely private, or to ensure that what is said about you is true. Each of these privacy concepts is potentially implicated here, as well as the additional idea that your privacy can be violated in ways that exploit you and violate your autonomy. *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 505-24 (2005); Ellen W. Clayton et al., *A Systematic Literature Review of Individuals' Perspectives on Privacy and Genetic Information in the United States*, 13 PLOS ONE e0204417, *14-18 (2018).

unlocking the secrets of our genomes, and yet the promised value of using genetic data to guide health care treatment is enormous.[15] Because there is a great deal of money to be made developing health care products that are tailored to individuals based on their genomic information (the goal of so-called "precision medicine"), many private and public research institutions would love to get their hands on large datasets of genetic information, especially when that information is coupled with multi-generational pedigrees, traits, and lifestyle choices. Analysts estimate the global market for precision medicine initiatives will increase from an estimated $92.4 billion in 2017 to $194.4 billion by 2024.[16] The value of the data that 23andMe and Ancestry store is colossal. There is, therefore, a great risk of deliberate data breaches or weak user privacy protections.[17]

By concentrating on law enforcement's use of FGG, and failing to address the larger risks of genetic research and disclosure, these privacy scholars miss the mark. Law enforcement's use of genetic genealogy to solve cold cases is a bogeyman. The larger threat to genetic privacy comes from shoddy consumer consent procedures used by DTC genetic companies, poor data security standards, and user agreements that permit rampant secondary uses of the users' DNA and data. Unless police drastically expand the way they are conducting genetic genealogical searches, there is too much fear and fascination surrounding this methodology. This Article seeks to demystify this unfounded fear.

This Article proceeds in three parts. In the first part, I explain the rise of genetic genealogical testing and how it is employed by police for FGG. I also clarify how FGG is different from a traditional search of the federal Combined DNA Index System (CODIS) database.[18] In the second part, I challenge the

---

15. Geoffrey Ginsburg & Kathryn Phillips, *Precision Medicine: From Science to Value*, 37 HEALTH AFF. 694, 694 (2018) ("The assembly of genomic, environmental, digital health, and patient-reported data from a variety of sources serves as the foundation for a powerful precision medicine platform that, when coupled to other national and global data and clinical networks, will lead to the dissemination of knowledge that will enable other health care delivery systems to benefit.").

16. *Global Personalized Medicine Market 2017-2018 & 2024: Market is Projected to Reach US$194.4 Billion by 2024 from an Estimated US$92.4 Billion in 2017*, PR NEWSWIRE (Oct. 15, 2018, 7:45 AM), https://www.prnewswire.com/news-releases/global-personalized-medicine-market-2017-2018--2024-market-is-projected-to-reach-us194-4-billion-by-2024-from-an-estimated-us92-4-billion-in-2017--300730848.html.

17. Yaniv Erlich & Arvind Narayanan, *Routes for Breaching and Protecting Genetic Privacy*, 15 NATURE REV. GENETICS 409, 409 (2014).

18. The Combined DNA Index System of the Federal Bureau of Investigation is commonly referred to as CODIS and is the federal database that contains the short-tandem repeat satellite markers at 13 or 20 non-coding

many concerns that scholars have raised in response to FGG. Specifically, I counter the arguments that it violates the Fourth Amendment, invades the privacy of innocent individuals, renders people unintentional genetic informants, improperly relies on police deception and the involuntary participation of suspects, and creates a *de facto* federal database. These concerns reflect misunderstandings of ordinary criminal procedure, the legal might of online user "agreements," and the distinctions between clinical research and criminal law. In the third part, I provide a unique theory for why we seem to fear "genetic informants." I conclude with a call for more nuanced policy measures that will better protect genetic privacy consistent with consumer expectations, while still permitting the use of FGG to deliver justice to victims and help convict serial killers and rapists.

II. THE EXPLOSION OF CONSUMER GENETICS

In the last few years, the cost for genetic testing has dropped considerably, and the large genetic ancestry companies have also lowered their prices, resulting in a predictable spike in demand.[19] One market leader, Ancestry, boasts over 15 million customers while its primary competitor, 23andMe, has more than 10 million customers.[20] One consumer genetics businessman remarked that "the inflection point [for DTC genetic test sales] started in the summer of 2016, and from there it's gone into the stratosphere."[21] Most of these sales have occurred in the United States, and roughly 1 in 25 Americans have had their samples analyzed online, without involving a physician or geneticist.[22] It is fair to say that the market for DTC genetic tests is booming.

---

regions for the individuals who have been sampled. The sampled population consists mostly of criminal offenders, but has been expanded to include arrestees. States may contribute to the federally-maintained database. *See* 34 U.S.C. § 40702 (2012).

19. Jie Yuan et al., *DNA.Land is a Framework to Collect Genomes and Phenomes in the Era of Abundant Genetic Information*, 50 NATURE GENETICS 160, 160 (2018); Tim Caulfield & Amy L. McGuire, *Direct-to-Consumer Genetic Testing: Perceptions, Problems, and Policy Responses*, 63 ANN. REV. MED. 23, 23 (2012); *see also* Bowen & Khoury, *supra* note 1.

20. *See About Us*, 23ANDME, https://mediacenter.23andme.com/company/about-us/; *Ancestry.com Surpasses 15 Million DNA Customers*, ANCESTRY, https://blogs.ancestry.com/ancestry/2019/05/31/ancestry-surpasses-15-million-dna-customers.

21. Antonio Regalado, *2017 Was the Year DNA Consumer Testing Blew Up*, MIT TECH. REV. (Feb. 12, 2018), https://www.technologyreview.com/s/610233/2017-was-the-year-consumer-dna-testing-blew-up.

22. *Id.*

However, the many DTC companies are considerably different from one another. Some offer tests that claim to match romantic partners based on their genetic soulmate, others create personalized travel holidays, and still others purport to identify favorite beverages, all based entirely on your genetic results.[23] Some even market themselves as being able to predict "how gay you are," by relying on a study that itself specifically dismissed the idea that their results could be used on individuals.[24] These kinds of tests lack clinical and analytic validity, and are a form of pseudoscience quackery.[25] Somewhere in the middle are health-related tests that claim to screen for food allergies or common drug side effects, with some following laboratory and privacy best practices, and others not. Then on the other end of the spectrum are the reputable DTC-companies such as 23andMe and Ancestry. These companies began by offering ancestry testing and have now branched out to offer health-related information.[26]

So far, it does not seem that finding out about an elevated risk for some disease changes behaviors, and in some cases it probably should not. The health-related risk information is often of very weak predictive value, particularly for complex diseases like cancer. Results often reflect small increases in overall lifetime risk, and cannot be interpreted without knowing someone's family history, personal risk, and environmental factors. Therefore, using DTC genetic tests to make health care decisions is often premature.[27] At present, it seems that most people pursue DTC genetic testing because they are tantalized by the idea of having as much information about themselves as possible, even information that has little predictive value.

A. Direct-to-Consumer Genetic Testing Companies are Under-Regulated and Provide Inadequate Consent and Privacy Protections

---

23. James W. Hazel & Christopher Slobogin, *Who Knows What, and When?: A Survey of the Privacy Policies Proffered by U.S. Direct-to-Consumer Genetic Testing Companies*, 28 CORNELL J.L. & PUB. POL'Y 35, 36–37 (2018).

24. Bizarrely, the app developers claimed it would be "absurd" for anyone to use the app in the way it was marketed, as its small-font disclosures technically warned that the app was not to be used to predict same-sex attraction. *See* Amy Maxmen, *'Gay Gene' App Provokes Fears of a Genetic Wild West*, 574 NATURE 609, 609 (2019).

25. Hazel & Slobogin, *supra* note 23.

26. *See* Megan A. Allyse et al., *Direct-to-Consumer Testing 2.0: Emerging Models of Direct-to-Consumer Genetic Testing*, 93 MAYO CLINIC PROC. 113, 116-117 (2018).

27. Jason Park et al., Question & Answer, *Privacy in Direct-to-Consumer Genetic Testing*, 65 CLINICAL CHEMISTRY 612, 613 (2019) (noting that "there is no solid evidence to support the contention that providing individuals with genetic information will . . . impact [their lifestyle choices].").

Because the DTC genetic testing industry is under-regulated, the quality of the privacy protections and clinical and analytic validity of the DTC genetic tests vary considerably.[28] This puts consumers at risk of data breaches with massive implications. Due to ineffective consent procedures at the initial stage when users submit a saliva sample and the failure of sites to require validation of user identities or to provide secure encryption, users may be unwittingly supplying the secrets of their genome to absolute strangers.[29] These strangers could then sell or share the valuable genetic profile data for legal (or illegal) insurance under-writing or pharmaceutical advertising schemes.

Importantly, there are no constitutional limitations on nefarious uses of data by private actors, and the federal Genetic Information Non-Discrimination Act (GINA) provides inadequate protection.[30] For example, GINA allows employers to use genetic risk information that they discover through "commercially available publications" such as newspapers, which might include websites like GEDMatch.[31] Further, GINA does not apply to life or disability insurance, and it requires that the discriminatory behavior be exposed. As with many forms of discrimination, detection is notoriously difficult, as is proving the intent behind the employer's or insurer's behavior. It is possible to argue that someone's insurance was priced the way it was or an adverse employment decision was made on some other pretextual, non-genetic basis. For example, in the context of racial discrimination, it is possible for an employer to successfully argue that the individual was fired due to very recent, and possibly fabricated, work performance issues, rather than due to the experience of racial bias. In the absence of data showing a disparate impact on a large number of employees, there is plausible deniability that the employer did not engage in intentionally unlawful employment discrimination. The same could occur with GINA. Finally, GINA is not written in stone; it is simply a Congressional statute that could be repealed. The privacy and security risks associated with DTC genetic testing led Senate Minority Leader Chuck Schumer (D-NY) to hold a press conference in 2017 to call for more regulatory oversight of DTC genetic

28. Hazel & Slobogin, *supra* note 23, at 40 ("DTC-GT remains largely unregulated in the majority of jurisdictions.").

29. Caitlin Curtis et al., *Protecting Trust in Medical Genetics in the New Era of Forensics*, 21 GENETICS MED. 1483, 1483-84 (2019) (proposing that "[i]t must not be possible for an individual to unwittingly sign an agreement that results in loss of control of their genetic data.").

30. *See* PROHIBITING EMPLOYMENT DISCRIMINATION ON THE BASIS OF GENETIC INFORMATION, 42 U.S.C. § 2000ff-1 (2019).

31. *Id.* at 42 U.S.C. § 2000ff-1(b) (2019).

testing.[32] Specifically, he asked the Federal Trade Commission to look closely at this industry and ensure that companies have fair privacy policies as well as adequate informed consent procedures. This has yet to occur.

This is big business and big data research—ancestry testing is just the gateway. Essentially, these companies are enormous biobanks. Because DTC genetic testing companies often also have pedigree and personal information, their genetic databases could be instrumental in assessing genetic risk for complex diseases. This makes their data incredibly valuable to pharmaceutical companies and clinical researchers, and Ancestry and 23andMe have publicized their relationships with these types of research bodies.

Unfortunately, the Common Rule, which provides protection for human subjects in research,[33] and the Health Insurance Portability and Accountability Act (HIPAA), which provides a bare minimum of protection for the security and privacy of identifiable health information,[34] do not apply to research that occurs outside of a health care setting and that is not federally funded.[35] Users may incorrectly expect certain health-related privacy regulations to apply because of the quasi-clinical nature of the information.[36]

Even if companies were to voluntarily comply with HIPAA, we cannot rely on existing laws to protect us because it is impossible to completely anonymize genomic information.[37] Every few months,

---

32. *Schumer Reveals: Popular at Home DNA Test Kits Are Putting Consumer Privacy at Great Risk, as DNA Firms Could Sell Your Most Personal Info & Genetic Data to All-Comers; Senator Pushes Feds to Investigate & Ensure Fair Privacy Standards for All DNA Kits*, CHARLES E. SCHUMER: UNITED STATES SENATOR FOR NEW YORK (Nov. 26, 2017), https://www.schumer.senate.gov/newsroom/press-releases/schumer-reveals-popular-at-home-dna-test-kits-are-putting-consumer-privacy-at-great-risk-as-dna-firms-could-sell-your-most-personal-info-and-genetic-data-to-all-comers-senator-pushes-feds-to-investigate_ensure-fair-privacy-standards-for-all-dna-kits.

33. 45 C.F.R. § 46 (2019).

34. 45 C.F.R. § 160 (2019); 45 C.F.R. § 164 (2019).

35. *See* Clayton et al., *supra* note 14, at *14 ("The U.S. Common Rule also permits the use of de-identified data without consent and with limited to no IRB oversight and endorses an expansive role for broad consent of identified data.").

36. Park et al., *supra* note 27, at 614-15 (discussing the risks of cyber-attacks to DTC genetic testing databases, such as those waged on the 100000 Genomes Project data in the United Kingdom).

37. This will be discussed in more detail below. Nora von Thenen et al., *Re-Identification of Individuals in Genomic Data-Sharing Beacons Via Allele Inference*, 35 *BIOINFORMATICS* 365, 365 (2019). *See also* Bridget F.B. Algee-Hewitt et al., *Individual Identifiability Predicts Population Identifiability in Forensic Microsatellite Markers*, 26 CURRENT BIOLOGY 935, 937 (2016) (finding that forensic markers have nontrivial ancestry information); Michael D. Edge et al., *Linkage Disequilibrium*

new methods are developed to use genetic datasets and public records to re-identify anonymized samples. Given the enormous potential of genetic information to reveal health risks in the future, we need to restrict access to this information in ways that might at first seem paternalistic. More will be said below about how we might improve the consent procedures and limit secondary uses, but we should also reconsider whether health-related information should *ever* be relayed without a physician's or genetic counselor's interpretation.

B. DTC Genetic Tests That Rely on SNP Data Reveal More Than Just Ancestry

The genetics revolution, fueled in part by an explosion in DTC genetic testing, is upon us. In 2017 alone, about 7 million genetic testing kits were sold directly to individuals, and 20 million kits were expected to be sold in 2018.[38] Driven mostly by genealogical hobbyists, the majority of the DTC ancestry genetic testing services rely on single nucleotide polymorphisms (SNPs), which are mutations at the level of the individual nucleotides. While SNP data is not nearly as rich as data gathered from sequencing, it still provides a significant amount of information about future risk of disease.

SNP data can also reveal whether users share segments of their genome with other users, predicting relatedness through a common ancestor. This works by analyzing the percentage of overlapping bits of genetic code, so-called "identical by descent" sections, that one shares with relatives. Assuming no historical inbreeding, one likely shares roughly 12% of their genome with first cousins, about 3% with second cousins, and less than 1% with third cousins.39 Thus, by finding and quantifying overlapping genetic regions, DTC companies can predict genetic familial relationships. However, because parents do not contribute exactly half of their genome to their offspring and the reshuffling of DNA can be random, third cousins may share more DNA fragments than second cousins.40 Since genetic inheritance varies from child to child, as one moves

---

Matches Forensic Genetic Records to Disjoint Genomic Marker Sets, 114 PROC. NAT'L ACAD. SCI. 5671, 5671-76 (2017) (finding that genetic databases can be compared to identify individuals).

38. Erlich et al., *supra* note 4 at 690; Park et al., *supra* note 27, at 612.

39. *Average Percent DNA Shared Between Relatives*, 23ANDME, https://customercare.23andme.com/hc/en-us/articles/212170668-Average-percent-DNA-shared-between-relatives (last visited Nov. 18, 2019).

40. Catherine Rehder et al., *American College of Medical Genetics and Genomics: Standards and Guidelines for Documenting Suspected Consanguinity as an Incidental Finding of Genomic Testing*, 15 GENETICS IN MED. 150, 151 (2013).

beyond the level of third cousins, there is a decent chance that a known genealogical relationship will not be detectable genetically.[41]

In addition to predicting genealogical relationships, some DTC genetic tests now reveal SNPs linked to developing diseases and other traits.[42] While most complex traits cannot be reliably and accurately predicted through SNP data, there are thousands of individual mutations or "genotypes" that can increase the likelihood of developing a particular trait or "phenotype." Some companies require a physician to order these test kits, but the most popular ones do not.[43] Other niche tests focus on so-called "recreational" traits like detecting the smell of asparagus in urine or identifying nutritional needs and possible food allergies.

The leading consumer genetics companies, 23andMe and Ancestry, allow consumers to download their raw genetic data in plain-text format, which can then be uploaded to third-party websites.[44] These websites provide a range of additional services, including interpreting the clinical relevance of mutations and allowing individuals to expand the reach of their genealogical search. Up to 62% of DTC customers will upload their genetic data to third-party websites for free or for a small fee.[45] One such third-party website is GEDMatch, an open-access service that is free for the most basic searches.[46]

C. Third-Party Sites Like GEDMatch Facilitate FGG

GEDMatch users can connect with even more distant relatives who used different testing services like FamilyTreeDNA or My Heritage. They do so by uploading their SNP profile, generated elsewhere, onto GEDMatch. The raw SNP data is analyzed using a simple algorithm, and the site then produces a list of likely relatives

---

41. Michael Edge & Graham Coop, *How Lucky Was the Genetic Investigation in the Golden State Killer Case?*, BIORXIV 5 (Jan. 29, 2019), https://www.biorxiv.org/content/biorxiv/early/2019/01/29/531384.full.pdf.

42. In 2013, the FDA sent cease and desist letters to 23andMe, ordering them to stop marketing and selling their health-related testing services until they received FDA approval for these devices. In 2017, the FDA approved 23andMe's carrier screening for hereditary Bloom syndrome, which created "DTC Testing 2.0." There was now precedent and a pathway for including disease-risk in the DTC panels. *See* Megan A. Allyse et al., *Direct-to-Consumer Testing 2.0: Emerging Models of Direct-to-Consumer Genetic Testing*, 93 MAYO CLINIC PROC. 113, 116-117 (2018).

43. Eline M. Bunnik et al., *Informed Consent in Direct-to-Consumer Personal Genome Testing: The Outline of a Model Between Specific and Generic Consent*, 28 BIOETHICS 343, 343-44 (2014).

44. Erlich et al., *supra* note 4, at 690.

45. *See* Maxmen, *supra* note 24, at 610.

46. *GEDmatch.Com Terms of Service and Privacy Policy*, GEDMATCH, https://www.gedmatch.com/tos.htm (last updated May 18, 2019).

automatically, without the need to share any underlying genetic information with the putative relative. In just a few years, GEDMatch has cultivated a large community of hundreds of thousands of users.[47] While the user agreements of 23andMe and Ancestry state that they will not disclose users' genetic data without a legal subpoena or warrant and that users must not submit samples under false identities,[48] GEDMatch's agreement has never included such guarantees. In fact, GEDMatch allows users to use an alias rather than their real names to register.[49] In 2018, GEDMatch made explicit in their user agreement that law enforcement could submit profiles from crime scene DNA to find a suspect's distant relatives.[50] Even before then, however, the GEDMatch user agreement included the following warning: "DNA and Genealogical research, by its very nature, requires the sharing of information. Because of that, users participating in this site should expect that their information will be shared with other users."[51]

In February 2019, FamilyTreeDNA announced that they too would allow law enforcement to submit crime scene DNA. Unlike GEDMatch, however, FamilyTreeDNA requires law enforcement to register all forensic samples and genetic files prior to uploading to the FamilyTreeDNA database. This is consistent with an interim policy issued by the Department of Justice (DOJ) in September 2019, which now requires law enforcement to submit the crime-scene derived profile explicitly on behalf of law enforcement, and not under false pretenses.[52] Permission to use FamilyTreeDNA's site for searching is only granted after the required documentation is submitted, reviewed, and approved. Permissible searches are limited to those identifying the remains of

---

47. Yuan et al., *supra* note 19, at 160.

48. *See 23andMe Guide for Law Enforcement*, 23ANDME, www.23andme.com/law-enforcement-guide (last visited Nov. 19, 2019) and *Ancestry Guide for Law Enforcement*, ANCESTRY, www.ancestry.com/cs/legal/lawenforcement (last visited Nov. 19, 2019).

49. "Although you may provide a real name for registration and data upload, you have the option of providing an alias for either login or data." *Terms of Service and Privacy Policy*, GEDMATCH, www.gedmatch.com/tos.htm (last updated May 18, 2019).

50. *Id.* ("When you upload Raw Data to GEDmatch, you agree that the Raw Data is one of the following: Your DNA… DNA obtained and authorized by law enforcement to either: (1) identify a perpetrator of a violent crime against another individual… [or (2)] identify remains of a deceased individual.").

51. Cyrus Farivar, *GEDmatch, a Tiny DNA Analysis Firm, Was Key for Golden State Killer Case*, ARS TECHNICA (Apr. 27, 2018), https://arstechnica.com/tech-policy/2018/04/gedmatch-a-tiny-dna-analysis-firm-was-key-for-golden-state-killer-case.

52. *Interim Policy: Forensic Genetic Genealogical DNA Analysis and Searching*, *supra* note 7.

a deceased individual or a suspect in a homicide, sexual assault, or trafficking case.[53]

In part because of these lax standards, law enforcement agencies have been uploading genetic profiles increasingly quickly to GEDMatch and FamilyTreeDNA to link unidentified criminals with relatives. Profiles are constructed from samples of blood, semen, or tissue found at the crime scene. Often there is insufficient DNA available from the crime scene to develop a full SNP profile or run multiple genetic tests.[54] However, law enforcement's ability to extract whole-genome genotypes from degraded crime-scene samples is improving.[55] Further, if there is enough cellular material, which is usually the case with semen from sexual assaults, law enforcement can use SNP microarrays.[56] The microarrays generate dense genetic profiles indistinguishable from those developed by the major DTC genetic testing companies.[57]

Because the identity of the person from whom the crime-scene sample came is often unknown, law enforcement uses a false name—"John Doe," for example—and submits it to GEDMatch. Then, when their "John Doe" matches someone in the database, they use genealogical data to determine a common ancestor who might be a great-great grandfather or grandmother. They then triangulate other data, such as birth, voting, and military records, to build out the pedigrees from that common ancestor, identifying all of the potential individuals who may be suspects. As we each have about 1,000 fourth cousins and 5,000 fifth cousins,[58] depending on the degree of relation, this process can be quite time-consuming. The methodology is known by different names. In the forensic genetics research community, it is referred to as "long-range familial searches" (LRFS). Law enforcement sometimes refers to this as Forensic Genetic Genealogy (FGG). This Article uses the term FGG.

The Golden State Killer, Joseph DeAngelo, was finally arrested using the FGG technique after eluding California police for

---

53. *Law Enforcement Guide*, FAMILYTREEDNA, https://www.familytreedna.com/legal/law-enforcement-guide (last visited Apr. 3, 2019).

54. New developments in massively parallel sequencing may be one way of getting more forensic data out of a limited amount of DNA in a sample. Denise S. Court, *Forensic Genealogy: Some Serious Concerns*, 36 FORENSIC SCI. INT'L: GENETICS 203, 203 (2018).

55. *See* Paul Ellenbogen & Arvind Narayanan, *Identification of Anonymous DNA Using Genealogical Triangulation* 5 (bioRxiv, Working Paper No. 531269, 2019).

56. Court, *supra* note 54.

57. Ellenbogen & Narayanan, *supra* note 55.

58. Court, *supra* note 54.

decades. DeAngelo murdered at least 12 people and sexually assaulted at least 45 women. Although law enforcement had multiple samples of his DNA from crime scenes, his DNA did not match any samples contained in the federal CODIS "offender" DNA database.[59] Until the advent of FGG, it seemed like the identity of the Golden State Killer might never be known, and justice for his many victims might never be delivered.

Once DeAngelo was finally arrested, questions regarding the method of his identification began to surface. The police reluctantly acknowledged that they used FGG, following the steps described above.[60] The profile derived from the crime scene matched someone in GEDMatch—a distant cousin of the perpetrator. With the help of genealogists, law enforcement found a common Italian ancestor shared by the Golden State Killer and his distant relative.[61] They then built the family tree branch by branch to find people who were about the right age and sex at the time of the crimes.[62] They initially tailed the wrong person, following him until he left some trash behind that contained his DNA, which they tested against the crime scene samples. It was not a match. They eliminated that individual and kept looking for other possibilities. Eventually, they identified Joseph DeAngelo. After analyzing DNA he also left on a piece of trash, they had their suspect. It was a match. The former cop, now in his early seventies, was finally arrested after evading law enforcement for decades.

The Golden State Killer was one of several suspects identified using FGG. Parabon® Nanolabs, Inc., a private company that has commercialized FGG for law enforcement, reports that a few dozen individuals have been arrested in this way.[63] Recently, another large forensic laboratory has entered the market.[64] Two decades after a man attacked ten women in their homes, investigators used FGG to identify Roy Charles Waller as the serial

---

59. More will be said about the database that the Federal Bureau of Investigations (FBI) maintains, CODIS, at p. 15. CODIS relies on a very different type of genetic profile, based on short-tandem repeats at 20 locations in the human genome that are not thought to code for traits. Because they are thought not to be coding regions, individual variation in these STRs is quite high, making them useful markers for differentiating individuals.

60. Edge & Coop, *supra* note 41.

61. Justin Jouvenal, *To Find Alleged Golden State Killer, Investigators First Found His Great-Great-Great-Grandparents*, WASH. POST (Apr. 30, 2018, 6:22 PM), https://wapo.st/2HCvivq.

62. *See* Guerrini, *supra* note 8, at *3.

63. Parabon's proprietary FDS methodology is called Snapshot Genetic Genealogy. *See Snapshot Genetic Genealogy*, SNAPSHOT, https://snapshot.parabon-nanolabs.com/genealogy (last visited Nov. 19, 2019).

64. Aldous, *supra* note 5.

rapist. Within five minutes of viewing the GEDMatch data, they identified a close relative of the perpetrator. Because the individual in the database was a close relative, the Sacramento police had a suspect in under two hours, and Waller was quickly arrested.[65]

The head of Parabon's genealogy department, CeCe Moore, predicts that hundreds of crimes will be solved using FGG in the coming years, assuming it continues to be legal.[66] While the cost of genotyping crime-scene DNA has dropped considerably, the method remains quite costly due to the significant manpower required to sift through archives to complete family pedigree charts. Few GEDMatch users are close relatives of perpetrators, as was the case in the Waller arrest. But when no other leads are available, FGG may reopen a cold case.

D. How FGG Differs from CODIS

1. The Federal NDIS and CODIS Database Maintained by the FBI

The DNA Identification Act of 1994 established the National DNA Index System (NDIS), which stores the DNA profiles contributed by federal, state, and local forensic laboratories.[67] All 50 states, the District of Columbia, the federal government, the U.S. Army Criminal Investigation Laboratory, and Puerto Rico contribute samples to the database.[68] The Act limits the categories of people whose profiles may be maintained in NDIS and details the quality assurance, privacy, and expungement requirements for participating laboratories. Once a match is identified by the CODIS system, the laboratories involved in the match share information to verify the match and identify the individual.[69] The only information contained in the CODIS database is an identifier of the contributing agency, a unique specimen identification number, the laboratory personnel associated with the analysis, and the "DNA profile."[70]

---

65. Heather Murphy, *How an Unlikely Family History Website Transformed Cold Case Investigations*, N.Y. TIMES (Oct. 15 2018), https://www.nytimes.com/2018/10/15/science/gedmatch-genealogy-cold-cases.html.

66. Antonio Regolado, *"Hundreds" of Crimes Will Soon Be Solved Using DNA Databases, Genealogist Predicts*, MIT TECH. REV. (Sept. 13, 2018), www.technologyreview.com/s/612001/hundreds-of-crimes-will-soon-be-solved-using-dna-databases-genealogist-predicts.

67. Frequently Asked Questions on CODIS and NDIS, FED. BUREAU OF INVESTIGATION, www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet (last visited Nov. 19, 2019).

68. *Id.*

69. *Id.*

70. *Id.*

2. The Limited Value of CODIS STRs for Things Other Than Identification

The DNA profile that CODIS employs is very different from the profile used to apprehend the Golden State Killer. The CODIS database uses short tandem repeats (STRs) to identify individuals.[71] STRs, also known as microsatellites regions of DNA, are between two and six nucleotides in length.[72] For example, in one area, a string of nucleotides such as "gata" might be repeated three times in one person (gatagatagata), but thirteen times in another. These STRs were chosen because they are polymorphic, meaning that there is significant genomic diversity between individuals at these locations. This yields more accurate matches, as it is very unlikely that unrelated people would share the same number of repeats at these loci.[73] Forensic laboratory technicians create a genetic profile from complete STRs that is thought to have a "vanishingly small," but not zero, probability of being shared with another person.[74] The STRs are in non-coding regions of the genome, so they are not directly involved in coding for proteins.[75] However, despite their limited clinical usefulness, it is not accurate to label the STRs as "junk DNA."[76]

The 20 STRs are not known to contain health-related information, making them much less useful for clinical research than data from SNPs. However, ancestry information can be gleaned from the CODIS markers.[77] Because the locations of genes are not random as once thought (a phenomenon called "linkage disequilibrium"), CODIS markers can be used to predict some health risks and identify genetic profiles from biobanks that match a record in the CODIS database.[78]

Initially, the DNA Profile in CODIS only included STRs at thirteen loci, but as of January 2017, the government gathers data at 20 loci to achieve even higher confidence in matching.[79] These

---

71. Daniel M. Bornman et al., *Short-Read, High-Throughput Sequencing Technology for STR Genotyping*, BIOTECHNIQUES 1, 1 (2012).

72. *Id.*

73. *Id.*

74. Susan Matheson, *DNA Phenotyping: Snapshot of a Criminal*, 166 CELL 1061, 1061 (2016).

75. The thirteen junk loci, or non-coding alleles, are "stretches of DNA that do not presently recognize traits and are not associated with any known physical or medical characteristics." Williamson v. State, 993 A.2d 626, 639 (2010).

76. Algee-Hewitt et al., *supra* note 37; Edge & Coop, *supra* note 41.

77. *See* Algee-Hewitt et al., *supra* note 37; Edge & Coop, *supra* note 41.

78. *See* Algee-Hewitt et al., *supra* note 37; Edge & Coop, *supra* note 41.

79. FED. BUREAU OF INVESTIGATION, *supra* note 67.

STR alleles are typically analyzed by amplifying the sample through multiplexed polymerase chain reaction, followed by capillary electrophoresis to separate segments.[80] This technique is time and cost-effective, but it does not allow for systematic genotyping of all STR loci.

Because the CODIS database relies on STRs at only 20 non-coding loci, there is not enough genetic information to provide matches to relatives beyond parents and siblings or to distinguish a fourth cousin from an unrelated person.[81] However, as most consumer genetics tests reveal hundreds of thousands of SNPs, identifying more distant relatives becomes possible—third cousins can usually be found, and many fourth cousins can be as well.[82] Because DOJ laboratories do not analyze SNPs during their forensic DNA casework, if they were to use this sort of analysis, it would need to be completed through an outside vendor laboratory.[83]
Even with SNP data, predicting an exact relationship based on shared DNA alone is not always possible, with the exception of identical-twin, parent-child, or full-sibling matches. There are certain relationships that produce similar patterns of shared DNA to each other. For example, a woman who shares 1750 centiMorgans (cMs) of DNA with you could be your half-sister, grandmother, granddaughter, or aunt. Likewise, a first cousin, grandchild, or a great-uncle/aunt/nephew/niece could all share roughly 950 cMs of DNA.[84] To predict the type of relationship, other sources of data such as age and death records would need to be used.

3. Familial Searching in CODIS Is of Limited Utility and Requires Additional Oversight

The FBI has discouraged law enforcement from using CODIS to identify partial STR matches. Partial matches occur when no one in the CODIS database matches the crime scene DNA at all 20 loci, but someone in the database matches at perhaps eight or so, indicating they probably are a sibling or parent of the person whose identity law enforcement is trying to determine. So-called "familial searching" in CODIS has been quite controversial, in part because this method produces a high rate of false positives. Also, like FGG, it identifies individuals by their association with people in the offender database, and not because they themselves chose to add

80. Bornman et al., *supra* note 71.
81. Edge & Coop, *supra* note 37, at 2-3.
82. *Id.*
83. DEP'T OF JUSTICE, *supra* note 52.
84. *The Limits of Predicting Relationships Using DNA*, THE DNA GEEK (Dec. 19, 2016), https://thednageek.com/the-limits-of-predicting-relationships-using-dna.

their DNA.[85] Conducting these familial searches under CODIS requires greater regulatory oversight, and is limited to "the most serious cases."[86] Because familial searches can be unreliable, many states, such as Colorado, have created a committee that determines when a familial match is suggestive enough to disclose it to local investigators. Some have argued that the additional layers of oversight for CODIS-mediated familial matches should also be required for FGG. Erin Murphy, a Professor of Law at New York University, for example, supports the separation between the local police and the state committee overseeing familial searches to "ensure that incidental findings, such as adoption or non-paternity, are distanced from those in close contact with the family." [87] However, in practice, there is often no investigative reason to disclose such information to relatives, and policies discouraging such disclosure are reasonable.

Law enforcement's use of private databases to identify criminals is viewed by some as an "alarming end-run"[88] around forensic databases like CODIS, given that CODIS has many more technical requirements for registering samples, conducting searches, and returning the results to investigating agencies.[89] This argument is misleading. In practice, law enforcement turns to DTC genetic databases only when CODIS does not result in a match, consistent with the recent interim policy on FGG issued by the DOJ. More importantly, FGG differs from CODIS in ways that makes it *more* permissible and less intrusive, and thus not an "end-run" at all. FGG might be avoiding some of the limitations on CODIS, but the limitations are not required outside of CODIS because of the way the comparison samples are obtained. The procedure does not require that the government obtains samples involuntarily from

85. "[F]amilial searches should be forbidden because they embody the very presumptions that our constitutional and evidentiary rules have long endeavored to counteract: guilt by association, racial discrimination, propensity, and even biological determinism." Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291, 304 (2010); *see also* Natalie Ram, *The Mismatch Between Probable Cause and Partial Matching*, 118 YALE L.J. POCKET PART 182, 185 (2009).

86. Erin Murphy, *Law and Policy Oversight of Familial Searches In Recreational Genealogy Databases*, 292 FORENSIC SCI. INT'L e5, e6 (2018).

87. *Id.*

88. *Id.* at e7.

89. "Thus, although corporations and individual citizens generate the largest storehouses of personal data today, the government—through its subpoena powers, contractual agreements, and public access to online data—can effectively bootstrap private information into its own domain without contending with the Constitution." Kimberly N. Brown, *Anonymity, Faceprints, and the Constitution*, 21 GEO. MASON L. REV. 409, 410 (2014).

individuals. With FGG, the government merely accesses a public genealogical database, albeit for forensic purposes.

a. The Data from DTC Genetic Databases Do Not Overlap with CODIS

The power of the FGG method lies in the sheer number of people who have contributed samples for DTC genetic tests. Data analysts project that a genetic database only needs to cover approximately 2% of the target population to "provide a third-cousin match to nearly any person."[90] Therefore, using population models that assume no inbreeding and random sampling of participants, researchers "predict that with a database size of ~3 million U.S. individuals of European descent…more than 99% of the people of [European] ancestry would have at least a single third-cousin match and more than 65% are expected to have at least one second-cousin match."[91] As the popularity of GEDMatch rises, and with FamilyTreeDNA announcing that they will allow forensic searching of their database, achieving this 2% target is within reach. With a warrant or subpoena, law enforcement could search 23andMe or Ancestry, which together already have tens of millions of users.[92]

b. FGG Uses Dense SNP Data, Which Contain Information about Disease Risk, Ancestry, and Physical Traits

Many of the panels that DTC companies employ are based on genome-wide association studies (GWAS) from thousands of unrelated individuals. Researchers look for point mutations on thousands of alleles and correlate them with disease risk. GWAS studies have transformed human genetics, with the discovery of thousands of mutations that are associated with increased (and in some cases decreased) risk of developing certain diseases. However, as members of the tested population likely have widely varying lifestyles and exposure to different environmental risks, the predictive effects for complex diseases are often small and in need of

90. Erlich et al., *supra* note 4. Others predict that with as little as 1% of the population genotyped with dense SNP data, accurate identification is possible in the "median" case. *See* Ellenbogen & Narayanan, *supra* note 55.

91. Erlich et al., *supra* note 4.

92. Ancestry.com's website states that AncestryDNA was "[l]aunched in May 2012, [and it] has more than 10 million people in its consumer DNA network, making it the largest in the world." *Ancestry Company Facts*, ANCESTRY, www.ancestry.com/corporate/about-ancestry/company-facts (last visited Nov. 18, 2019). From 23andMe's website, it states that "23andMe has more than 5,000,000 customers." *About Us*, 23ANDME, https://mediacenter.23andme.com/company/about-us (last visited Nov. 18, 2019).

updating.[93] Even so, GWAS studies have the unusual scientific feature of being highly reproducible.[94] The ability to make disease-risk predictions from GWAS studies makes the data from the SNP microarrays, specifically those used by law enforcement in FGG, much more rich and sensitive. [95]

c. FGG Corrects the Racial Bias Inherent in the CODIS Database

There is another important way in which the genealogical databases differ from CODIS. The CODIS database is racially biased, due to its significant over-sampling of African Americans. [96] At least 40% of CODIS is comprised of African Americans, making it much more likely that they, and their family members, will be implicated in a crime through a profile in CODIS. Familial partial match searches would render about 17% of the African American population identifiable, as compared to just 4% of the Caucasian population, despite much lower base rates of African Americans in the general population.[97]

In contrast to CODIS, the consumer genomics databases are much more likely to represent individuals from Northern Europe, thus providing matches for the mostly Caucasian population.[98] Thus, the racial bias of the databases goes in opposite directions, with CODIS oversampling people of color, especially African Americans, and consumer genomics oversampling Caucasians from Northern Europe. Because the consumer genomics databases do not overlap significantly with samples gathered pursuant to CODIS regulations, they provide a rich source of leads for many more suspects who are not of African American descent.

---

93. The predictive ability of risk evaluation from GWAS studies "depends on the number and effect size of the loci associated with the probability of developing a given phenotype, and has to date been found to generally be modest for most multifactorial conditions." Joel Krier et al., *Reclassification of Genetic-Based Risk Predictions as GWAS Data Accumulate*, 8 GENOME MED. 1, 2 (2016).

94. Urko Merigorta, Replicability and Prediction: Lessons and Challenges from GWAS, 34 TRENDS IN GENETICS 504, 504 (2018).

95. Murphy, *supra* note 86, at e5.

96. Curtis, *supra* note 29, at 2; *see also* Henry T. Greely et al., *Family Ties: The Use of DNA Offender Databases to Catch Offenders' Kin*, 34 J.L. MED. & ETHICS 248, 258-259 (2006) (noting that African American suspects are four to five times more likely to be identified through CODIS searches than white Americans).

97. Greely et al., *supra* note 96, at 259.

98. Yuan, *supra* note 19, at 162-163.

E. FGG Does Not Require a Warrant

1. FGG Is Not a Return to the Abhorrent General Warrant

The Fourth Amendment prohibits the government from conducting unreasonable searches of people or their property.[99] The Framers of the Constitution sought to prevent the abhorrent royal practice of general warrants, where the government could harass people by "ransack[ing] one's personal belongings" to find evidence for a prosecution.[100] Is FGG a return to the general warrant, as it gives police the power to conduct "fishing expeditions" of innocent distant relatives of criminals in non-forensic databases? There is obvious appeal to this sort of thinking. The idea of a surveillance state that can search innocent people to solve crimes offends our deeply-held notions of liberty and privacy. However, there is a very important distinction between the historical practice of general warrants and the use of FGG that shows just how unlike the general warrant FGG truly is.

Before the government may search a person or place in a way that could pose an unreasonable risk to their privacy, they must first obtain a warrant from a judge or magistrate based upon probable cause.[101] The officer applying for a warrant must describe with particularity the place to be searched and the persons or things to be seized. Warrants thus limit the scope of searches and prevent boundless ransacking. Any evidence, or the fruits of that evidence, unconstitutionally seized from that defendant and thus obtained in violation of the Fourth Amendment's strictures is inadmissible.[102]

No search occurs unless the individual "manifested a subjective expectation of privacy in the searched object, and society is willing to recognize that expectation as reasonable."[103] Following

---

99. U.S. CONST. amend. IV.

100. United States v. George, 975 F.2d 72, 74 (2d Cir. 1992); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2239 (2018) ("The American colonists echoed this reasoning in their 'widespread hostility' to the Crown's writs of assistance—a practice that inspired the Revolution and became '[t]he driving force behind the adoption of the [Fourth] Amendment.'") (internal citation omitted; alterations in original).

101. U.S. CONST. amend. IV.

102. Alderman v. United States, 394 U.S. 165, 176 (1969).

103. Kyllo v. United States, 553 U.S. 27, 33 (2001) (internal quotations omitted). This formulation comes from Justice Harlan's concurring opinion in *Katz v. United States*, 389 U.S. 347, 361 (1967). ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and,

this, the Supreme Court has repeatedly held that the Fourth Amendment does not protect "[w]hat a person knowingly exposes to the public."[104] Relatedly, a warrant is not required in many cases where someone voluntarily shares their otherwise private information with third parties. Under the "third-party doctrine," it is presumed that making a deliberate choice to share information waives the individual's privacy interest in the once-private information.[105] However, what one "seeks to preserve as private," even in public, may justify constitutional protection.[106]

2. For Fourth Amendment Purposes, Discarded DNA Has Regrettably Been Analogized to Trash

The Supreme Court followed the principles laid out in the previous section in *California v. Greenwood*, where it stated that "society would not accept as reasonable [a] claim to an expectation of privacy in trash left for collection in an area accessible to the public."[107] This case proved to be very beneficial to law enforcement, particularly with regard to surreptitiously obtaining DNA to test against crime scene samples. Many state courts have analogized to *Greenwood* to permit the collection of genetic samples from discarded water

---

second, that the expectation be one that society is prepared to recognize as 'reasonable.' Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited."). The simplicity of the language belies how fraught its interpretation has become. Fourth Amendment scholar Orrin Kerr has argued that "[a]lthough the courts speak of a single 'reasonable expectation of privacy' test, the one label masks several distinct but coexisting approaches. Four approaches predominate, together reflecting four different models of Fourth Amendment protection." Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 506 (2007). Kerr argues that only one of the four descriptive models, "the probabilistic model," is actually concerned with the privacy expectations of ordinary citizens. *Id.* Other scholars, on the other hand, argue that each of Kerr's four models boil down to an evaluation of intrusiveness. *See* Bernard Chao et al., *Why Courts Fail to Protect Privacy: Race, Age, Bias, and Technology*, 106 CAL. L. REV. 263, 277–78 (2018); *see also* Christopher Slobogin, *Proportionality, Privacy, and Public Opinion: A Reply to Kerr and Swire*, 94 MINN. L. REV. 1588, 1603-04 (2010).

104. *Katz*, 389 U.S. at 351; *see also* Kevin J. Schrop, *Your Cooperation is Greatly Appreciated: The Fourth Amendment, National Security Letters, and Public-Private Data Sharing*, 122 PENN ST. L. REV. 849, 857–58 (2018).

105. *See Carpenter*, 138 S. Ct. at 2216 (2018); *see also* Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

106. *Katz*, 389 U.S. at 361.

107. 486 U.S. 35, 41 (1988).

bottles, gum, and sealed envelopes.[108] The theory is that the DNA on the trash is *also* trash, and is knowingly shared with third parties. This analysis strains credulity given a) how little most people know about the feasibility of pulling a genetic profile from their water bottles or chewing gum; b) the vast amounts of private, immutable information contained in that DNA profile, containing secrets that are still being unlocked; and c) our inability to refrain from shedding DNA on personal items we must eventually discard (unless we create a public health disaster by never recycling anything or disposing of our trash). It is indefensible to suggest that someone loses their subjective expectation of privacy in their genetic material by leaving a soda can in the trash or in a public recycling bin. Nevertheless, many state courts have made precisely these claims, relying on analogies to trash from *Greenwood*.[109]

Raynor v. Maryland provides a particularly alarming example of how states may treat "discarded" DNA.[110] In *Raynor*, the defendant had agreed to be questioned in police custody in connection with a rape investigation.[111] Detectives asked him to provide a DNA sample, and he refused. While he was sitting in the chair, they noticed that he kept scratching his bare arms. They

---

108. Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U.L. REV. 857, 865 (2006) ("With abandoned DNA, existing Fourth Amendment law appears not to apply at all. It may be that an individual harbors an actual expectation of privacy in his genetic information. The few reported cases involving abandoned DNA have followed Greenwood's analysis, though, and have concluded that there is no objective expectation of privacy in saliva—and the DNA contained within it--that is left behind on a coffee cup or on a smoked cigarette.").

109. For example, in *Commonwealth v. Ewing*, the police gave the defendant—then the suspect—a meal, soft drink, straw, and cigarettes during questioning at a police station. 85 N.E.2d 993,1000 (Mass. App. Court. 2006), *aff'd*, 873 N.E.2d 1150 (Mem) (Mass. 2007). The police took some of the defendant's discarded items to the crime lab for DNA testing, where DNA on the cigarette butt matched that found in the rape kit. *Id.* at 1001. The defendant moved to suppress the DNA test. *Id.* at 1000. The court held that the defendant had no reasonable expectation of privacy to the cigarette butt he discarded, as he voluntarily abandoned it as trash. *Id.* at 1001. Regardless of whether the police conduct was a ruse, police are allowed to conduct "ruses" so long as there is not coercion. Here, the defendant was offered a meal, which he accepted. "Under the circumstances, the ruse, if it was one, was proper." *Id.* New Hampshire, by contrast, has opted to protect individual privacy to a greater extent under its state constitution, rejecting the idea that individuals relinquish their expectation of privacy in the trash they discard for municipal collection. State v. Goss, 834 A.2d 316, 319 (N.H. 2003) ("We conclude that the defendant exhibited an actual expectation of privacy in his trash because he placed it in black plastic bags with the expectation it would be picked up by authorized persons for eventual disposal. We also conclude that society is prepared to recognize that expectation as reasonable.").

110. Raynor v. State, 99 A.3d 753, 755 (Md. 2014).

111. *Id.*

figured he might have shed some skin cells. After he left the room, detectives obtained his genetic material from his chair, tested it to develop a genetic profile, and compared the genetic profile to that of DNA obtained from the crime scene.[112] The Maryland Court of Appeals held that law enforcement's "analysis of the 13 identifying loci within [defendant's] DNA left behind on the chair at the police station, in order to determine a match with the DNA the police collected from the scene of the rape, was not a search" under the Fourth Amendment.[113] The basis for these sorts of opinions (i.e., the idea that one loses her subjective expectation of privacy when she leaves articles in the trash) has become increasingly vulnerable. The doctrine appears to be on thin ice.[114]

3. Consumers Who Upload Genetic Profiles to Open-Access Genetic Websites Lose Their Subjective Expectation of Privacy

In the recent Fourth Amendment case of *Carpenter v. United States*, the majority opinion recognized that the type and volume of information, as well as the manner in which it is shared with third parties, should be relevant to our actual subjective expectation of privacy.[115] It may no longer be enough that the information is technically "shared" by placing it somewhere others can access. Indeed, the *Carpenter* majority recognized a "world of difference" between the limited information collected by telephone companies when users dial a landline telephone number and the "exhaustive chronicle" of cellphone-site location information that is "casually" shared by subscribers.[116] The court noted that just as cell-site tracking information is "detailed, encyclopedic, and effortlessly compiled … generat[ing] increasingly vast amounts of increasingly precise [data]," the very same could be said for genetic information gathered through shed DNA.[117] The methods for determining ancestry, health, and familial information from our genomes are becoming much more precise, cheap, and predictive. At the same time, the donor of the DNA sample has done nothing deliberate to share her DNA with law enforcement. DNA collection may be as casual as picking up a coffee cup that someone throws away in the trash and swabbing it.

---

112. *Id.* at 756.
113. *Id.* at 759.
114. *See* Erin Cooper, Comment, *Following in the European Union's Footsteps: Why the United States Should Adopt Its Own "Right to Be Forgotten" Law for Crime Victims*, 32 JOHN MARSHALL J. INFO. TECH. & PRIVACY L., 2015, 185, 195–96.
115. 138 S. Ct. 2206, 2215 (2018).
116. *Id.* at 2219.
117. *Id.* at 2212, 2217.

Further, the Court reminded us that the "nature" of the information sought matters for the third-party doctrine as well.[118] Each week, scientists discover new information that is embedded in our genome. While predictions are imperfect given varying genetic penetrance (i.e., the likelihood the phenotype will develop from the genotype) and expression (i.e., the degree to which the phenotype, once it develops, is expressed), there are thousands of highly penetrant disease risks that we can gather from our genes.[119] And we cannot change the genes we are born with—at least not yet. Genetic information is, therefore, much more sensitive and in need of privacy protection than are cell-site location records. Thus, if the Court were asked to determine whether the analysis of discarded DNA constitutes an unreasonable search under *Carpenter*, the outcome might be very different today than it would have been under *Greenwood*. Indeed, even the dissents in *Carpenter* made plain their disfavor for *Greenwood*, with Justice Gorsuch excoriating it as one of the many "unbelievable" results of the "unpredictable" *Katz* test.[120] In rejecting the idea that people lose their subjective expectation of privacy when they discard trash, Justice Gorsuch's dissent suggests that the *Greenwood* majority canvassed the "habits of raccoons" rather than the "habits of the country."[121]

However, there is an essential difference between cell-site location tracking, searching involuntarily discarded DNA, and voluntary uploading of genetic information to sites like GEDMatch or FamilyTreeDNA. Namely, the act of sharing is much more active and deliberate in the latter case. In holding that law enforcement required a warrant before they could obtain cell-site location data from wireless companies, the majority in *Carpenter* questioned whether cell-site tracking information is truly voluntarily shared consistent with the third-party doctrine.[122] For one, cellphones are "such a pervasive and insistent part of daily life" that carrying one is nearly obligatory in modern society.[123] The Court reasoned it would be a huge inconvenience to ask someone to abstain from using a cellphone in order to protect their geographic expectations of privacy. This argument is even stronger when thinking about whether we voluntarily discard our DNA through skin cells or hair. We cannot opt out of possessing or shedding our DNA. It would

---

118. *Id.* at 2216.

119. Caroline F. Wright et al., *Assessing the Pathogenicity, Penetrance, and Expressivity of Putative Disease-Causing Variants in a Population Setting*, 104 AM. J. HUMAN GENETICS 275, 275 (2019).

120. *Carpenter*, 138 S. Ct. at 2266 (Gorsuch, J., dissenting).

121. *Id.*

122. *Id.* at 2220.

123. *Id.*

require substantial and unreasonable efforts to scrub all of our discarded hair, fingernails, or skin cells.[124]

However, we *can* opt out of participating in genetic genealogical services, and we can certainly avoid exposing our genetic information to strangers on open-source websites. The people who have uploaded their SNP profiles to GEDMatch or FamilyTreeDNA might not fully appreciate the massive amounts of information they are sharing. However, they are sharing this information affirmatively, and voluntarily, through a website for genealogical hobbyists. So far, this is all that the third-party doctrine requires. Unlike cell-site tracking, which occurs "without any affirmative act on the user's part beyond powering up,"[125] uploading a genetic profile to a website like GEDMatch requires several deliberate and voluntary steps. If the Court continues to pursue doctrine like that in *Carpenter*, the truly voluntary sharing of profiles—by providing a saliva sample, receiving genetic results, downloading them in plain-text format from 23andMe, registering one's name or alias at a separate site, and finally uploading one's data to that site—would easily distinguish cell-site tracking from FGG.

4. FGG is Analogous to the Warrantless Searching of Publicly-Accessible Peer-to-Peer Networks to Prosecute Child Rape

Cases involving the prosecution of people who disseminate child pornography (which is a euphemism for child rape) may be instructive in predicting how the doctrine might apply to investigations that use FGG. Law enforcement commonly identifies violations of child pornography laws by searching for digital signatures (SHA-1) on files that are known to contain pornographic images of children.[126] When perpetrators download or share these files on peer-to-peer networks like Gnutella or Limewire, they can be traced through their digital signatures. Investigators use something called the "Wyoming Toolkit" to scan Gnutella and

---

124. Thus, it does seem that the Supreme Court should evaluate the cases using *Greenwood* to analogize DNA to trash and should reconsider whether a warrant ought to be required before a presumptively innocent individual has their DNA obtained from a discarded coffee cup or door handle.

125. *Carpenter*, 138 S. Ct. at 2220.

126. JOHN WESLEY HALL, JR., 2 Search and Seizure § 51.01 (5th ed. 2019) LexisNexis; *see also*, *e.g.*, *New Technology Fights Child Porn by Tracking Its "PhotoDNA,"* MICROSOFT NEWS (Dec. 15, 2009), https://news.microsoft.com/2009/12/15/new-technology-fights-child-porn-by-tracking-its-photodna.

Limewire for profiles sharing illicit content.[127] The Wyoming Toolkit is a computer program and database that automatically identifies and labels child pornography shared over the Internet through peer-to-peer file sharing networks.[128]

Those prosecuted for owning or distributing child pornography have argued that the use of the Wyoming Toolkit without a warrant constitutes an unconstitutional search under the Fourth Amendment. Some have even analogized to the thermal image scanning at issue in *Kyllo v. United States*[129] to argue that searching the reference dataset against the peer-to-peer networks violated reasonable expectations of privacy.[130] State and federal courts have considered this issue and "none [have] found an expectation of privacy" in the files that are retrieved from one's personal computer that one has uploaded to a publicly accessible, peer-to-peer network.[131] As such, there has been no search. Even highly sensitive information, the possession of which is a strict liability crime, may be deemed "no longer private" when shared through a third-party website. This is the case even where the users would need to search for this content using specific codes like "PTHC" (which represents the phrase "preteen hardcore").[132]

It is a simple step to move from these cases to an easy defense of FGG. Even if the genetic information uploaded is something meant to be kept private due to its sensitive nature, one loses the expectation of privacy when uploading this data from a private computer to a peer-to-peer sharing site like GEDMatch.

5. There Are No Vicarious Rights Under the Fourth Amendment

Even if the Court were prepared to require a warrant for searching sites like GEDMatch, there would be other obstacles to vindicating any Fourth Amendment rights. The remedy for a Fourth Amendment violation is the exclusion, in an eventual criminal trial, of any evidence that was improperly obtained as a result of the

---

127. Jay Shapiro, *Obtaining and Suppressing Identification*, 1 THE PROSECUTION AND DEFENSE OF SEX CRIMES § 21.03 (2019), LexisNexis.

128. State v. Roberts, 2015 UT 24, ¶ 1, 345 P.3d 1226, 1230 (Utah 2015).

129. 533 U.S. 27, 29 (2001).

130. *Roberts*, 2015 UT 24, ¶ 25, 345 P.3d at 1231.

131. *Id.* (collecting cases). *See also* United States v. Hill, 750 F.3d 982, 986 (8th Cir. 2014) ("[A] defendant has no reasonable expectation of privacy in files…retrieved from his personal computer where [the defendant] admittedly installed and used LimeWire to make his files accessible to others for file sharing.") (internal quotations omitted).

132. United States v. Driver, No. 11-20219, 2012 WL 1605975, at *2 (E.D. Mich. May 8, 2012).

unconstitutional search.[133] Because this is the remedy, the right only inheres to criminal defendants for unconstitutional searches of *their* person or things. Thus, even co-conspirators who were "aggrieved solely by the introduction of damaging evidence" cannot assert a Fourth Amendment claim unless they either owned or had an expectation of privacy in what was searched.[134]

As applied to FGG, this means that the innocent relatives whose genetic profiles were searched through GEDMatch would certainly have no "standing" to bring a Fourth Amendment claim.[135] While the Supreme Court has referred to this as "standing," that term is not quite right. This requirement is neither jurisdictional nor rooted in Article III of the Constitution, but rather "is more properly subsumed under substantive Fourth Amendment doctrine."[136] Essentially, because there is no remedy for the non-defendants whose data were searched, there is no Fourth Amendment right that is violated.[137] This also means that the Golden State Killer, and other defendants like him, cannot borrow the Fourth Amendment violations of others and assert them by proxy. Fourth Amendment rights are *personal* rights, which "may not be vicariously asserted."[138]

a. FGG Is Unlikely to Provide Basis for a Relative's Invasion of Privacy Claim

---

133. *Wong Sun v. United States,* 371 U.S. 471, 484–85 (1963).

134. Alderman v. United States, 394 U.S. 165, 171–72 (1969).

135. "[T]here is no standing to contest a search and seizure where, as here, the defendants: (a) were not on the premises at the time of the contested search and seizure; (b) alleged no proprietary or possessory interest in the premises; and (c) were not charged with an offense that includes, as an essential element of the offense charged, possession of the seized evidence at the time of the contested search and seizure." Brown v. United States, 411 U.S. 223, 228–29 (1973).

136. United States v. Noble, 762 F.3d 509, 526 (6th Cir. 2014).

137. As Shima Baradaran-Baughman aptly notes, this sort of analysis is flawed, as courts focus on the personal rights of the criminal defendant who often do not have "clean hands." Instead, courts should balance the rights not just of the criminal defendant *ex post*, but also of society *ex ante*, presuming that the search is of an innocent individual. The rights-holder "represents the rights of all of society, yet the information before the court often relates only to the individual defendant." Shima Baradaran, *Rebalancing the Fourth Amendment*, 102 GEO. L.J. 1, 3 (2013). However, even if courts were prepared to balance the privacy interests of all of society, *ex ante*, it does not work as well in this context. When a search for a match with crime-scene DNA is conducted, the DNA donor is still innocent until proven guilty. Nonetheless, he has a huge evidentiary hurdle to overcome, given that his semen or blood was found at the crime scene; this no doubt skews the privacy analysis to the DNA and its donor, whose hands are "dirty." *See* Bernard Chao et al., *supra* note 103, at 281–82.

138. *See Brown*, 411 U.S. at 230 (1973); Simmons v. United States, 390 U.S. 377, 389 (1968).

A criminal suspect's relative, who presumably uploaded her profile to GEDMatch, could theoretically try to assert a civil claim for invasion of privacy against law enforcement.[139] It could be a regular tort suit, if she could overcome governmental immunity.[140] Or, it could be a federal statutory claim, if she could assert that law enforcement acted under the color of state law when violating her civil rights.[141] However, if she was indeed the person who uploaded or "published" her own genetic profile, she would have no recourse for public disclosure of private facts or any other conceivable privacy actions.[142] The plaintiff must maintain an expectation of privacy in the information that is disclosed or the database that is surveilled to prevail on any of the relevant privacy torts.[143] Evidence that the plaintiff voluntarily submitted the once-private information to a publicly available database would render her privacy claims moot. If, however, someone else submitted her profile on her behalf and without her consent, there could be a privacy tort against that individual. While the amount of saliva required by 23andMe (about a teaspoon) makes it difficult to obtain a sample without the individual's compliance, it is currently possible for parents to submit samples on behalf of their children, Other DTC companies only require a cheek swab.[144] One genealogical message board even provides guidance for how to force an elderly person to submit a sample, by "adding a small amount of sugar to the tip of the tongue."[145] The criminal whose DNA was uploaded by law enforcement under an alias, however, would not have a cause of action in tort, as courts have uniformly concluded that criminals have no reasonable expectations of privacy in the DNA they leave at crime scenes.[146]

---

139. *See* Rakas v. Illinois, 439 U.S. 128, 133–34 (1978); Monroe v. Pape, 365 U.S. 167 (1961).

140. "In some jurisdictions, sovereign immunity prohibits an individual from suing the state for invasion of privacy. In other jurisdictions, sovereign immunity imposes no such bar because it has been waived via the state's applicable tort claims act." Lior Jacob Strahilevitz, *Reunifying Privacy Law*, 98 CAL. L. REV. 2007, 2016–17 (2010).

141. *See* 42 U.S.C. § 1983 (2019).

142. 103 AM. JUR. PROOF OF FACTS 3d 159 (Originally published in 2008).

143. *See* Anonsen v. Donahue, 857 S.W.2d 700, 702–03 (Tex. App. 1993).

144. *Providing Saliva Sample for DNA Test Kit*, 23ANDME, https://customercare.23andme.com/hc/en-us/articles/202904530-Providing-Saliva-Sample-for-DNA-Test-Kit (last visited Nov. 18, 2019); *Who Can Use the 23andMe Kit*, 23ANDME, https://customercare.23andme.com/hc/en-us/articles/202904520-Who-can-use-the-23andMe-kit.

145. *Genealogy and Family History Beta*, Comment to How to Get an Elderly Person to Provide Saliva Sample for DNA?, STACKEXCHANGE, https://genealogy.stackexchange.com/questions/12177/how-to-get-an-elderly-person-to-provide-saliva-sample-for-dna.

146. Samuel D. Hodge, Jr., *Current Controversies in the Use of DNA in Forensic Investigations*, 48 U. BALT. L. REV. 39, 61 (2018).

Opponents of FGG argue that the practice violates both the rights of the criminal defendant and the rights of the family member who contributed her genetic profile to GEDMatch. Understanding who holds the right proves to be critical for Fourth Amendment analysis. The distant relative has no Fourth Amendment claim if she is not prosecuted for a crime based on that DNA evidence. Likewise, the criminal defendant has no Fourth Amendment claim if the uploaded DNA comes from the crime scene and law enforcement uses it solely to identify the perpetrator.

F. Debunking the Common Privacy Critiques of FGG

Many critics of FGG now acknowledge that it does not violate current understandings of the Fourth Amendment.[147] Even if the search through FGG passes constitutional muster, however, many argue that the methodology is too intrusive into the lives and genomes of innocent people, because it (1) improperly renders distant family members "unintentional informants," (2) improperly encourages deceptive investigative methods by law enforcement, and (3) is a *de facto* and impermissible universal database. I will address each of these concerns in turn. After much consideration, I conclude that each concern is based on some form of genetic essentialism. There are many traditional non-genetics cases, which involve methodologies similar to FGG in important ways, that do not give rise to any legal claims and are in fact generally considered appropriate searches or disclosures. The privacy alarms that many critics of FGG have sounded seem to reflect a misunderstanding of how traditional criminal cases are investigated, when privacy rights are violated, and how ordinary testimony is obtained.

1. Being Precise About the Actual Privacy Costs

In general, many of the public responses to the apprehension of the Golden State Killer questioned whether the cost to privacy was just too high to justify the use of FGG. One ethicist recognized that the killer "was a horrible man and it is good that he was identified," but wondered whether "the end justif[ied] the means?" [148] Others echoed these sentiments, noting the "tendency in such

147. Ram, *supra* note 12 ("Current Fourth Amendment precedent, meanwhile, is unlikely to bar warrantless police searches of genealogical DNA databases.").

148. Gina Kolata & Heather Murphy, *The Golden State Killer is Tracked Through a Thicket of DNA, and Experts Shudder*, N.Y. TIMES (Apr. 27, 2018),

cases to minimize the privacy costs because the gains are so great."[149] In the popular press, FGG has been described as alternatively "creepy"[150] and "dystopian."[151] The sponsor of a bill in the Maryland legislature to ban the use of FGG expressed his concerns this way: "If the state doesn't want law enforcement searching databases full of its criminals, why would it allow the same kind of search conducted on citizens who haven't committed any crimes?"[152]

But what *exactly* are the privacy costs? Initially, it seems horribly offensive that the government could use a family member's DNA to track down a distantly related criminal. But why, exactly? After all, when law enforcement exploited GEDMatch to apprehend the Golden State Killer, the database was used to do precisely what it was designed to do—reduce the anonymity of users and connect them with their distant relatives. Of course, law enforcement's use of the database was probably not contemplated by its users, and submitting a crime scene-derived sample through an alias requires deceit. But GEDMatch (and now FamilyTreeDNA) users seek information about relatives of whom they have no knowledge. If these services only confirmed the names and identities of close relatives whose identities and personal histories were known, they would offer nothing of value. Importantly, law enforcement ostensibly only use the profile to find people who shared a common ancestor with the perpetrator, and do not compare any other SNP information. They simply use the database to connect the user with crime scene DNA.

From the perspective of the users, they have to expect and be open to the idea that uncovering their pedigree could reveal

---

www.nytimes.com/2018/04/27/health/dna-privacy-golden-state-killer-genealogy.html.

149. Matt Ford, *How the Supreme Court Could Rewrite the Rules for DNA Searches*, THE NEW REPUBLIC (Apr. 30, 2018), https://newrepublic.com/article/148170/supreme-court-rewrite-rules-dna-searches.

150. Megan Molteni, *The Creepy Genetics Behind the Golden State Killer Case*, WIRED (Apr. 27, 2019), www.wired.com/story/detectives-cracked-the-golden-state-killer-case-using-genetics.

151. Avi Selk, *The Ingenious and 'Dystopian' DNA Technique Police Used to Hunt the 'Golden State Killer' Suspect*, WASH. POST (Apr. 27, 2018), www.washingtonpost.com/gdpr-consent/?destination=%2fnews%2ftrue-crime%2fwp%2f2018%2f04%2f27%2fgolden-state-killer-dna-website-gedmatch-was-used-to-identify-joseph-deangelo-as-suspect-police-say%2f%3futm_source%3dreddit.com&utm_source=reddit.com&utm_term=.63486f10d5a4.

152. Megan Molteni, *Should Cops Use Family Tree Forensics? Maryland Isn't So Sure*, WIRED (Feb. 6, 2019), www.wired.com/story/maryland-considers-banning-genetic-genealogy-forensics.

unpleasant information about their relatives or their past. Indeed, learning that you are a distant relative of a serial killer is probably much less traumatic than discovering that your biological parents are not who you thought they were, or that you were conceived by rape or incest.[153] These sorts of revelations seem much more likely to be unexpected or surprising, and yet are known to occur through many forms of DTC genetic testing. The possibility for learning this type of information does not stop DTC genetic testing in its tracks, so we cannot be worried about the revelation of disturbing information from our pedigrees. Indeed, there is no indication that the relatives in the Golden State Killer case were even informed that it was their SNP data that led to the arrest.

The privacy concerns in the Golden State Killer case cannot simply be that a GEDMatch user discovered unpleasant information about a distant relative, as that is part of the service that 23andMe and Ancestry offer. What must be troubling, then, is the government's involvement in their discovery. But the government is not forcing innocent people to upload their genetic profiles to the internet. They are merely providing those already desirous of a more complete family tree with an even *more* complete family tree—that is, if they even tell the user about the connection with the crime-scene DNA. In many cases, there is no reason for law enforcement to reveal pedigree information with the relatives whose genetic profiles were used to find a common ancestor, unless they want to ask them questions about their relatives to narrow the pool of suspects. Once they have the pedigree information from a site like GEDMatch, they could presumably delete the fake account created from the crime-scene DNA.

The critics of FGG shift from critiquing the government's search, to critiquing the criminal's involuntary submission of his DNA, to critiquing the GEDMatch user's uploading of their DNA, which implicates their family members in crime. While all of these are valid *potential* privacy violations, in order to assert them, critics need to be a bit sloppy about what exactly the FGG technology entails. When we focus on precisely what is being searched and whose privacy interests are at stake, the privacy concerns about FGG largely disappear. Much of this disagreement about what to

153. Sarah Zhang, *When a DNA Test Shatters Your Identity,* THE ATLANTIC (July 17, 2018), www.theatlantic.com/science/archive/2018/07/dna-test-misattributed-paternity/562928 ("But not all biological parents want to be found. In conversations and correspondence with more than two dozen people for this story, I heard of DNA tests that unearthed affairs, secret pregnancies, quietly buried incidents of rape and incest, and fertility doctors using their own sperm to inseminate patients. These secrets otherwise would have—or even did—go the grave.").

focus on stems from confusing the pedigree with the underlying DNA that predicted it and from confusing a presumptively innocent individual with the donor of crime-scene DNA. While the donor of crime-scene DNA, obtained through a rape kit, is still innocent until proven guilty, he will often have to use a *mens rea* defense rather than being able to refute the *actus reus*. For this and other reasons, criminals have few privacy rights in crime-scene DNA, which is what is used to search GEDMatch. This next section aims to sharpen our focus of what exactly is being searched, disclosed, and violated when law enforcement uses FGG.

2. Defendants Who Are Prosecuted Through FGG Did Not Volunteer to Have Their Samples Contributed

The first big problem with FGG, according to opponents, is that those arrested following a search of GEDMatch or FamilyTreeDNA did not volunteer to have their DNA included in those databases. Further, the users of GEDMatch also did not "specifically and knowingly consent to the use of their genealogical data by law enforcement."[154] Of course, before these sites updated their terms of use, those uploading their data to GEDMatch did not give explicit consent to its particular use by police. But that is somewhat irrelevant. They gave blanket consent to all potential uses, by virtue of uploading their data to a public access site. Just as I consent to *all* uses of my videos when I upload them without conditions to YouTube or Facebook, I cannot later claim a privacy violation if someone used my public video in a way I had not specifically contemplated. The same is true in this context. The fact that users did not provide specific consent to a particular use is immaterial, given that they consented to all uses.

One team of researchers went so far as to call law enforcement's methods "unethical," as they "bypassed the codes of informed consent."[155] Informed consent in the medical context requires that a patient understands what is being done to her before she agrees to be touched by a physician or researcher. Failure to provide informed consent could result in battery or medical malpractice liability. The concept of the defendant's consent is under-theorized in criminal law. Detectives ought to do better to make sure that defendants actually consent to procedures that require it. But let me be clear: prosecutors will never be required to obtain "informed consent" before accessing a suspect's data, nor should they be.

---

154. Curtis et al., *supra* note 29, at 1483.
155. Court, *supra* note 55.

The reasons for informed consent in the medical world have to do with the trust that patients place in their physicians, the need to make sure that their autonomy is respected, and the need to protect them from unnecessary harm.[156] Informed consent also recognizes the inherent power and information imbalance between the patient and the physician.[157] The concern is that the baseline relationship is paternalistic, since a patient might just go along with whatever the skilled physicians suggests. Given the trust that consumers place in the DTC companies and labs that process sensitive, health-related information, some researchers have sensibly argued for informed consent for DTC genetic testing.[158] I discuss this below in Part I.

Prosecutors, on the other hand, have a very different sort of relationship to the perpetrators of crime, which is inherently adversarial and not based on trust. The power and information imbalance swings in the opposite direction, at least at the beginning of an investigation where the perpetrator holds all of the cards. At this point, it is the prosecution that is playing catch-up. Given that it is crime-scene DNA that is being analyzed under FGG, and not a search of a *presumptively innocent individual*, the donor of the crime-scene DNA sits in a very different posture than a disempowered and autonomy-seeking patient. There is simply no reason to afford him the kind of arms-length respect for autonomy that clinical informed consent necessitates.

True, the suspect has never been arrested or convicted of a violent crime, which would have placed his DNA in CODIS. But that hardly means that "the identification of individuals who are not directly included in a genetic database runs afoul of any given reason law enforcement use of such databases is legally and ethically

156. "The first is that patients are generally persons unlearned in the medical sciences and therefore, except in rare cases, courts may safely assume the knowledge of patient and physician are not in parity. The second is that a person of adult years and in sound mind has the right, in the exercise of control over his own body, to determine whether or not to submit to lawful medical treatment. The third is that the patient's consent to treatment, to be effective, must be an informed consent. And the fourth is that the patient, being unlearned in medical sciences, has an abject dependence upon and trust in his physician for the information upon which he relies during the decisional process, thus raising an obligation in the physician that transcends arms-length transactions." Cobbs v. Grant, 502 P.2d 1, 9 (1972).

157. Janet Dolgin & Lois Shepherd, BIOETHICS AND THE LAW 45–46 (Wolters Kluwer Aspen Casebook Series, 3d. ed. 2013) (discussing the history and principles of informed consent to health care).

158. Bunnik et al., *supra* note 43.

acceptable."[159] The justifications for CODIS are different because they *need* to be different to satisfy the Fourth Amendment.[160]

The inquiry into the propriety of FGG begins and ends with the consent of the initial user by their uploading data to an open-access website. Yes, this consent implicates others, which will be discussed below in Part H. But there is simply no Fourth Amendment right of privacy in something uploaded for *anyone* to view. Outside the context of a Fourth Amendment search, the justifications can be, and need to be, different. That does not mean that the justifications for FGG are inconsistent with those for CODIS or that the former runs afoul of the latter. By using non-forensic, public databases, detectives are certainly taking advantage of the law and dodging the warrant requirement. But justifications for FGG need not mirror those given for searching CODIS, just as the justifications for searching a peer-to-peer site for child pornography may be less rigorous than the justifications for searching someone's private computer. With CODIS, there are necessary limitations because the government *mandates* submission of samples. It is entirely predictable that the calculation is different with FGG (requiring less justification) than with CODIS (requiring more justification).

a. We Do Not Possess Privacy Rights in Our Pedigree

Opponents of FGG seem to confuse pedigree relationships with the genetic regions of homozygosity that revealed them. FGG employs the GEDMatch algorithm to find a percentage of shared genetic material, which in turn predicts relationships. But there is nothing inherently private in our pedigree, especially when viewed from the perspective of someone actively seeking pedigree information.

Even if the distant relative were told that her GEDMatch profile linked her to a suspected serial killer, it is hard to see how this revealed private information. It is potentially embarrassing and sensitive. But is it private, just because it was unknown? Many vital statistics and records are public. In the ordinary course and absent a closed adoption, we do not have a reasonable expectation of privacy

159. Ram, *supra* note 11.

160. *See* Maryland v. King, 569 U.S. 435 (2013) (holding that conducting a DNA swab test as a part of the arrest procedure does not violate the Fourth Amendment because the test serves a legitimate state interest and is not so invasive so as to require a warrant. The routine administrative procedures that occur during a booking for an arrest do not require the same justification and the search of a location).

in our pedigree.[161] If my cousin visited the genealogical archives in Salt Lake City, Utah, and through a search of public military, property, voting databases and birth records, discovered that our great uncle had deserted the army in the Korean War, and then disclosed this information on her social media account, would this constitute "private" information that was revealed? Under tort law, the answer is no. I might not have known this information, but legally, obscurity is not the same as privacy.

If instead we focus on the disclosure that the person to whom we are related is a likely rapist and serial killer, this is also not private information. Joseph DeAngelo had three daughters and a granddaughter.[162] Could any of them successfully argue that their privacy rights were violated when the Sacramento County police held a press conference to claim that Joseph DeAngelo, their close relative, was a suspected murderer and rapist? And if they could not claim that disclosing this fact violated their privacy, then how could an even *more* distant relation? If all that was "revealed" by the investigation was the relationship, it is hard to imagine that these distant cousins possess a privacy right that is greater than those even closer in relation to the suspect. Viewing the pedigree information this way, the FGG did not reveal *any* private information at all.

b. While It Is Not Perfect, FGG May Actually Reduce Surveillance of Innocent People

Opponents of FGG are also concerned that it will result in police "taking samples from various members of the family tree, even though they aren't suspects."[163] Indeed, in the Golden State Killer case, the police took DNA surreptitiously from two suspects who

---

161. Of course, the legal rights that attach are very different from interpersonal expectations, as many families seek to keep pedigree information private. One might argue that those seeking to keep pedigree information private should have to overcome a rebuttable presumption that this information should not be allowed to be private. Courts could employ something like a "best interests" test, adopted from family law, to determine whether disclosure of pedigree information would result in a net harm to the child. Examples of when that might not be disclosed until maturity might include incidents of incest or rape.

162. Avi Selk, *All We Know About Joseph DeAngelo, the Golden State Killer Suspect Who Became a Suburban Grandfather,* WASH. POST (Apr. 26, 2018), www.washingtonpost.com/news/post-nation/wp/2018/04/26/joseph-deangelo-golden-state-killer-suspect-was-normal-grandpa-according-to-teen/?utm_term=.d186d54572a2.

163. Oreskes et al., *False Starts in Search for Golden State Killer Reveal the Pitfalls of DNA Testing*, L.A. TIMES (May 4, 2018), www.latimes.com/local/lanow/la-me-ln-golden-state-killer-dna-20180504-story.html.

proved to be innocent.[164] False leads will certainly lead to testing genetic samples to exclude, rather than include, people as suspects. But on balance, will FGG obviously lead to more harassment of innocent individuals? Given the alternative methods of investigation, such as DNA Dragnets,[165] high-pressure interviews, and regular surveillance, it does not seem so. The trick is for law enforcement to use the most reliable FGG and genealogical methods to home in on as few targets as possible and then quickly obtain a warrant to collect genetic samples from them.

A case that opponents of FGG often cite as a cautionary tale involves a very different form of "familial matching" than that used by FGG. A filmmaker, Michael Usry, Jr., was wrongly arrested for the murder of an 18- year-old girl in Idaho Falls.[166] Police uploaded crime-scene DNA to a small publicly-searchable database, YSearch, previously owned by Ancestry.[167] Using Y-chromosome testing, the crime-scene DNA yielded a "partial match" with Michael Usry Jr's father. Y-chromosome testing is different from the dense autosomal SNP profile now used by 23andMe, Ancestry, and GEDMatch. It produces haplotype group data that runs in a patrilineal line, connecting us to the ancestors of our deep, deep past. Because of this, connections can be quite remote, and unlike FGG, do not suggest a recent common ancestor. Y-chromosome matching is useful when there is a mixture of male-source and female-source DNA, and law enforcement wants to isolate the male DNA.[168] However, this method of ancestry testing is not very precise and is no longer used by CODIS for offender matching. This is because "men with matching Y-profiles are related in extended patrilineal clans, many of which may not be represented in a given database."[169] Thus, the partial match in this case was much weaker than would be a finding that two individuals share significant portions of their autosomal DNA through SNPs.

---

164. *Id.*

165. Manfred Kayser, *Forensic DNA Phenotyping: Predicting Human Appearance from Crime Scene Material for Investigative Purposes*, FORENSIC SCI. INT'L: GENETICS, Sept. 2015, at 33. DNA Dragnets can be carried out in communities where no DNA profile match is obtained through CODIS. In these cases, hundreds or thousands of individuals who live near the crime are asked to "volunteer" to provide a saliva sample for STR profiling through CODIS. Non-participation might invite suspicion, and thus direct investigators toward following up with that individual. Also, participation by the suspect's close relatives can allow for a partial or distant match, especially if the suspect is a male and Y-chromosome STRs are used instead of autosomal STRs.

166. Molteni, *supra* note 150.

167. *Id.*

168. Mikkel Andersen & David Balding, *How Convincing Is a Matching Y-Chromosome Profile?*, 13 PLOS GENETICS e1007028 (2017).

169. *Id.*

Even so, despite this weak partial match, law enforcement used very weak circumstantial evidence of Usry's connection to Idaho, and the fact that he made a film about a grisly murder, to deem Usry the chief suspect. After obtaining a warrant to have YSearch provide the name of the partial match, police arrested and detained Usry for over a month.[170] He was ultimately cleared through a direct comparison of his DNA to the crime-scene DNA.[171] This is a deeply concerning outcome. This case exposes the potential for misusing weak genetic matching data, in conjunction with very little circumstantial evidence, to detain someone for far too long. Usry cannot get this time back, and even though he was cleared of the charges, those who read about his arrest might always be suspicious.

The problem here, however, is not unique to FGG. False arrests and false leads are inevitable in any investigation. Far from trampling on privacy rights, FGG and other DNA methodologies may actually *reduce* invasions of privacy and biased prosecutions by law enforcement. Without solid physical evidence like a DNA match, investigations and prosecutions are often left to the discretion of law enforcement, who must often rely on unreliable sources of information such as telephone tip-lines, eyewitness testimony, or psychological profiles. A DNA match through FGG also reduces the need for intrusive investigations of the innocent, which might include quasi-voluntary DNA Dragnets[172] and eliminate the implicit or explicit racial biases that impact investigations.[173]

If the prosecutor's office is aggressive and a jury can be convinced, weak evidence can lead to many wrongful convictions. Methods such as FGG, combined with DNA Phenotyping,[174] provide a more efficient and less discretionary means of apprehending suspects in many murder and sexual assault cases.[175] In addition to protecting the rights of the innocent, it also means that

---

170. Molteni, *supra* note 150.

171. Crimesider Staff, *Privacy Concerns After Public Genealogy Database Used to ID "Golden State Killer" Suspect*, CBS NEWS (Apr. 27, 2018), www.cbsnews.com/news/privacy-concerns-after-public-genealogy-database-used-to-id-golden-state-killer-suspect.

172. Victor Toom et al., *Approaching Ethical, Legal and Social Issues of Emerging Forensic DNA Phenotyping (FDP) Technologies Comprehensively*, FORENSIC SCI. INT'L: GENETICS, May 2016, at c2 (questioning the truly voluntary nature of each person's contribution of their sample for a DNA Dragnet, given the suspicion that may be aroused from non-submission).

173. Brief DNA Saves et al. as Amici Curiae Supporting Petitioner at 18-19, State of Maryland v. King, 548 U.S. 435 (2013) (No. 12-207).

174. *See* R. Williams & M. Wienroth, *Social and Ethical Aspects of Forensic Genetics: A Critical Review*, 29 FORENSIC & SCI. REV. 145, 146-147 (2017).

175. *See* Ray A. Wickenheiser, *The Business Case for Using Forensic DNA Technology to Solve and Prevent Crime*, 7 J. BIOLAW & BUS. 34, (2004), www.dnaresource.com/documents/BusinessCaseforDNA.pdf.

justice will more likely be served for the many victims of violent crimes.

3. Debunking the Claim that Law Enforcement Cannot Lie When Investigating Cases

Critics of FGG have questioned law enforcement's use of FGG to arrest Joseph DeAngelo, claiming they deceived GEDMatch by submitting the Golden State Killer's DNA under a false name.[176] Others have gone one step further, suggesting that the investigators' use of a fake identity to upload the crime-scene DNA profile to GEDMatch might raise questions about the legality of the evidence.[177] Though we may not like it, law enforcement consistently engages in deception when investigating crimes. In some cases, due to the trickery of the perpetrators of crime, it might be necessary to use similar countermeasures to arrest them. As deception may even be used to encourage, if not coerce, a confession of a crime, it is certainly constitutional when applied to deceiving the rest of society.[178]

For example, in *Holland v. McGinnis*,[179] an officer lied about the strength of the evidence against the defendant, which in part caused the defendant to confess. The court held that this lie alone was insufficient to make the confession involuntary, as it did not "overcome Holland's will by distorting an otherwise rational choice of whether to confess or remain silent." [180] The Court went on to say that "[o]f the numerous varieties of police trickery … a lie that relates to a suspect's connection to the crime is the least likely to render a confession involuntary."[181]

---

176. Court, *supra* note 55.

177. Kolata & Murphy, *supra* note 148. In September of 2019, the Department of Justice issued an interim policy on Forensic Genetic Genealogy (FGG), which prohibits investigations under the jurisdiction of the federal DOJ from submitting a crime-scene derived SNP profile under false pretenses to a DTC company or third-party site like GEDMatch. This may not be as restrictive as suspected, given that GEDMatch and FamilyTreeDNA explicitly permit law enforcement to submit profiles for forensic purposes. DEP'T OF JUSTICE, *supra* note 52.

178. *See* Frazier v. Cupp, 394 U.S. 731, 739 (1969). In *Frazier*, the Supreme Court held that police deception is a relevant factor in determining whether or not a confession is voluntary, but that it must be analyzed under the totality of the circumstances to see whether the deception violated due process. The Court concluded that "[t]he fact that the police misrepresented the statements [the codefendant] had made is, while relevant, insufficient in our view to make this otherwise voluntary confession inadmissible." *Id.*

179. 963 F.2d 1044, 1051 (7th Cir. 1992).

180. *Id.*

181. *Id.*; *see also* People v. Rubio, 911 N.E.2d 1216, 1235 (Ill. App. 2 Dist. 2009). ("[M]isrepresentations, of course, may cause a suspect to confess, but

Trickery is also legal when law enforcement uses it to obtain DNA samples for identification purposes. In *Commonwealth v. Ewing*,[182] police gave the defendant cigarettes, a meal, and a soft drink, with the hope of collecting and testing his discarded DNA. The police pulled a DNA profile from the cigarette butt that matched DNA from the rape kit. The defendant moved to suppress the evidence "because it was the product of an illegal ruse."[183] The Court, in finding that the defendant had no reasonable expectation of privacy in the DNA from the cigarette butt, confirmed that "[t]he police have been permitted to employ a ruse [even] to gain entry into a [person's] home in certain situations…There was no evidence of coercion. Under the circumstances, the ruse, if it was one, was proper."[184] Many other state courts have held similar ruses, specifically to obtain DNA, are constitutional.[185]

Detectives may also impersonate others to obtain DNA samples from suspects. For example, in *State v. Athan*, police officers pretended to be attorneys at a fake law firm.[186] They sent the defendant a letter, asking him to join a fictitious class action lawsuit.[187] Athan believed the request to be true and returned the letter. Law enforcement pulled a DNA profile from the envelope, which Athan presumably licked when sealing it. Athan was arrested for murder based on this DNA sample, and he moved to suppress all incriminating DNA evidence. The court held that obtaining the saliva sample in this case did not violate the defendant's constitutional rights. Law enforcement officers have also been permitted to lie to defendants to get them to submit a DNA sample to exonerate them from a fake crime.[188] However, if the State's manipulation or deception goes too far and is found to have improperly coerced the defendant, the consent to providing the DNA sample will be void.[189]

---

causation alone does not constitute coercion; if it did, all confessions following interrogations would be involuntary because "it can almost always be said that the interrogation caused the confession.").

182. 67 Mass. App. Ct. 531, 540, *aff'd*, 449 Mass. 1035 (2007).

183. *Id.*

184. *Id.* (internal quotation marks omitted).

185. *See* Piro v. Guyer, No. CV 08-372-M-BLW, 2010 WL 985735, at *1 (Idaho Mar. 15, 2010); State v. Christian, 723 N.W.2d 453 (Iowa Ct. App. 2006); Marino v. Commonwealth, 488 S.W.3d 621, 622 (Ky. Ct. App. 2016); People v. Sterling, 869 N.Y.S.2d 288, 290 (2008); People v. LaGuerre, 815 N.Y.S.2d 211 (2006).

186. 158 P.3d 27, 31 (Wash. 2007).

187. *Id.*

188. *See* Wynche v. State, 987 So.2d 23, 24 (Fla. 2008).

189. *See* State v. McCord, 833 So.2d. 828, 829 (Fla. Dist. Court. App. 2002).

Detectives may also impersonate inmates or co-conspirators to procure confessions. In *Illinois v. Perkins*,[190] the defendant made incriminating statements to an undercover officer who was posing as a fellow inmate in the prison. The defendant was incarcerated for a burglary, but the police suspected he was involved in an unrelated murder. The defendant moved to suppress the incriminating statements he made to the undercover cop. The Court held that coercion is determined from the perspective of the suspect, and the Fifth Amendment right to remain silent does not protect a suspect from boasting of criminal activity in front of people they think are cellmates.[191]

Law enforcement officers are allowed to engage in deception and subterfuge to identify criminals for prosecution.[192] Given the extent of this permitted conduct, it seems quite unlikely that the use of false names to submit samples to GEDMatch would render this evidence inadmissible. Even so, the recently issued DOJ guidance on the use FGG states that law enforcement should always identify themselves when submitting samples, and that they should not do so under an alias.[193] As FamilyTreeDNA and GEDMatch now explicitly allow forensic use, this does not seem like a big obstacle. To be clear, this is not to say that police deception should be encouraged or that it is even ethical, and the analysis of discarded DNA *should* but does not require a warrant. Instead, this Article merely suggests that the critique of police deception through FGG will fall flat in the courtroom. The evidence will not be excluded because detectives submitted the DNA sample to GEDMatch under a false name. There is substantial case law to support the use of deception, even vis-à-vis criminal defendants. Here, the deception was toward a private entity, which was not the subject of the investigation. As a result, this is even more likely to pass constitutional muster. Because our guiding light in these analyses is the Constitution, ironically the privacy rights of innocent parties are even less protected than those of the criminal suspect.

4. Debunking the Claim That Informants Must Be Asked First Before Providing Inculpatory Information

190. 496 U.S. 292 (1990).

191. *Id.* at 297-98.

192. Confessions obtained through the use of subterfuge are not vitiated so long as the methods used are not of a type reasonably likely to procure an untrue statement. *See* C.T. Drechsler, *Annotation, Admissibility of Confession as Affected by Its Inducement Through Artifice, Deception, Trickery, or Fraud*, 99 A.L.R.2D 772, 783 (1965).

193. DEP'T OF JUSTICE, *supra* note 52.

Several critiques of FGG contend that it is unfair to force individuals to unknowingly become informants against their distant relatives.[194] An early article on the topic stated "fierce objections" to FGG, as privacy advocates "maintain that it turns family members into genetic informants without their knowledge or consent."[195] Given the amount of deception that is permitted under the Fifth and Fourteenth Amendments, it is not surprising that to be admissible, incriminating information need not be voluntarily and intentionally shared. Providing more examples outside the genetics context might help make this clearer.

The DTC genetic testing users who uploaded their genetic information online "to facilitate self-discovery" probably had no idea, up until last year, that they could become "criminal informants vis-à-vis their own families."[196] Of course, if a DTC genetic company claimed not to share genetic information without a warrant or court order and then shared this information in violation of its terms of service, the user could sue for breach of contract. But GEDMatch and other databases were so attractive to law enforcement because their terms of service implicitly, and then explicitly, allowed this sort of use. There is a reason that detectives did not attempt to search 23andMe or Ancestry: their terms of service would not allow it, at least not without a court order or subpoena.

However, the critique is not that GEDMatch violated its terms of service. Rather, the claim here seems to be that law enforcement should not be allowed to use deception to turn family members against one another, without their consent. The subtext of the question "did you realize you could be an unintentional informant against your family member?"[197] suggests that prosecution witnesses are ordinarily asked whether they would like to provide incriminating testimony.

---

194. "People who submit DNA for ancestors testing are unwittingly becoming genetic informants on their innocent family," Steve Mercer, the chief attorney for the forensic division of the Maryland Office of the Public Defender, told the Associated Press. "[Such users] have fewer privacy protections than convicted offenders whose DNA is contained in regulated databanks," he said. Nancy Dillon, *Cops Tracked Down Golden State Killer With Genealogy Website That Keeps Users' Genetic Info Public*, N.Y. DAILY NEWS (Apr. 28, 2018), www.nydailynews.com/news/crime/public-genealogy-website-led-golden-state-killer-arrest-article-1.3958936.

195. Selk, *supra* note 151.

196. Guerrini, *supra* note 8.

197. *See* Matthew Feeney, *"Genetic Informants" and the Hunt for the Golden State Killer*, THE CATO INSTITUTE, CATO@LIBERTYBLOG (Apr. 30, 2018, 4:11 PM), www.cato.org/blog/genetic-informants-hunt-golden-state-killer.

Any criminal defense attorney will tell you this is not how it works. Instead, it goes something like this: a cop knocks on your door after your next-door neighbor is murdered, asks whether he can come in and ask you a few questions, then pulls out a notepad and begins probing you for details. He might ask questions like "when was the last time you saw your neighbors, how close were you, and did they fight?" In the course of answering these questions, you might inadvertently provide incriminating evidence against the victim's husband. You mention that you saw him in the driveway cleaning out the trunk of his Subaru from about 5:00pm-6:00pm. You know this because you were watching your favorite TV show at the time, and this is when you popped your head out the window to see from where the vacuum sound was coming. Your neighbor, the husband, told the police he was alone at a movie theater at this time. The medical examiner puts his wife's death at about 5:00pm that evening. Your testimony shatters the husband's alibi. Whether or not your testimony will be admissible will not hinge *at all* on whether you were asked first whether you were intending to incriminate the suspect.

Quite simply, we do not have a right to be asked first before we provide incriminating testimony against others. We possess rights against self-incrimination due to the Fifth Amendment. But a prosecution witness's testimony is not rendered inadmissible just because she gave the testimony before realizing that it would be incriminating.

5. Debunking the Claim That FGG Is a De Facto Universal Database

Critics of FGG have also argued that it creates a shadow, *de facto* universal federal genetics database, populated with our private information that we never agreed to share. They argue that if we think law enforcement should be allowed to use FGG to arrest criminals, then we should have an open conversation about the propriety of a population-wide database, which some already recommend on privacy and fairness grounds.[198] However, if a

198. Elizabeth Joh, *A Consumer DNA Testing Company's Alarming New Marketing Pivot*, SLATE (Mar. 29, 2019, 4:26 PM), https://slate.com/technology/2019/03/familytreedna-dna-testing-solve-crimes-law-enforcement.html; In response to law enforcement's use of FGG, some criminal law and privacy advocates have suggested we instead adopt a universal genetic forensic database, accessible only through a warrant. For a serious proposal for a universal forensics genetic database, *see* James Hazel et al., *Is it Time for a Universal Genetic Forensic Database*?, 362 SCIENCE 898, 899-900 (2018).

universal, forensic database is the goal, they say, "we should arrive there directly, not as a *de facto* matter."[199]

But by asking whether we would be okay with a database like this, established by the federal government, opponents of FGG sidestep the crucial aspect of this methodology.[200] These databases are not "established" by the government. The databases are not created, stored, or maintained by the government. Individuals are freely, voluntarily, and enthusiastically populating these non-governmental databases. This distinction matters and needs to be given more weight.

Consider when someone posts pictures of you on social media without your consent. Parents are the worst offenders, posting so many pictures of their non-consenting children that there is now a term for this: "sharenting."[201] One group of researchers discovered that of the 25,727 photographs parents posted on Facebook, 75.5% of those inspected contained a child between the ages of 0 and 8 years old.[202] Nearly 40% of parents posted over 100 photos of their child.[203] The large majority of these pictures also contained information such as the child's name and birthdate, which along with the location of their birth could be sufficient to predict their social security number.[204] By posting information about children, who cannot consent, parents are creating a digital footprint that might have unforeseen consequences.[205] Even so, it would be strange to claim that these pictures could not be accessed by law enforcement if they were to become relevant to a child welfare case.

In addition to Facebook asserting a license in posted photos,[206] courts have recognized that "Facebook itself does not guarantee privacy."[207] Courts have held that "generally, the photographs posted on a social networking site are neither privileged nor protected by any right of privacy, regardless of any privacy

---

199. *Id.*

200. Ram, *supra* note 12.

201. Anna Brosch, *When the Child is Born Into the Internet: Sharenting as a Growing Trend Among Parents on Facebook*, NEW EDUC. REV. 225, 229 (2016).

202. *Id.*

203. *Id.*

204. Alessandro Acquisti & Ralph Gross, *Predicting Social Security Numbers from Public Data*, 106 PROC. NAT'L ACAD. SCI. U.S.A. 10975, 10975 (2009); *see also* Brosch, *supra* note 201.

205. Brosch, *supra* note 201, at 234.

206. "While the person taking the picture may retain a copyright, Facebook users grants Facebook 'a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any content that [the user] post[s] on or in connection with Facebook.' This means that Facebook can license a user's content to others freely without obtaining any other approval from the user. Once a user's pictures or videos are shared on Facebook, the content remains in backup copies." *See* Jessica Ronay, *Adults Post the Darndest Things: (Ctrl + Shift) Freedom of Speech to (Esc) Our Past*, 46 U. TOL. L. REV. 73, 86 (2014).

207. Nucci v. Target Corp., 162 So. 3d 146, 154 (Fla. Dist. Ct. App. 2015).

settings that the user may have established."[208] If we do not have privacy rights in the "sharenting" photos parents post, then what about photographic evidence that raise suspicions of criminal activity?

Somewhat shockingly, criminals often share information about their crimes on social media. Sometimes, photographs include images of co-conspirators, holding guns or drug paraphernalia on a public street, or boasting about the "hit" they just did.[209] Whether or not the photograph is staged or real, posting these sorts of images is reckless, as prosecutors can use them to prove aspects of any criminal case. Specifically, they may be used to claim that the defendants are members of a gang, which may increase their sentence.[210] If I am a co-conspirator in the picture who never agreed to have my photo taken, and in fact vehemently protested it being uploaded to Instagram, do I have a right for it not to be used against me? The answer is no. Instagram, Facebook, and Twitter are not *de facto* government databases. They are public and semi-public data warehouses, with scores of once-private information that law enforcement can exploit. The use of GEDMatch is not that different from a Facebook user with lax privacy settings, whose posts all default to "public." If detectives search that user's Facebook profile and find incriminating photographs or posts, they are not doing an "end-run" around the Fourth Amendment. They are taking advantage of a legal source of data.

6. Debunking the Claim That Individuals Do Not Want to Participate in GEDMatch to Help Solve Cold Cases

While we probably should not rely on what consumers want when crafting privacy policies, as many are unaware of privacy risks,[211] it is simply not the case that most Americans find FGG creepy and dystopian. Banning FGG denies many people the opportunity to assist in cracking cold cases. While many speculate

---

208. *Id.* at 153-54.

209. *See Post, Shoot*, INVISIBILIA (Mar. 15, 2019, 3:03 AM), www.npr.org/templates/transcript/transcript.php?storyId=700738025; *see also* Aaron Leibowitz, *Chicago Public Schools Monitored Social Media for Signs of Violence, Gang Membership,* PROPUBLICA (Feb. 11, 2018, 4:00 AM), www.propublica.org/article/chicago-public-schools-social-media-monitoring-violence-gangs.

210. Tony Rizzo, *Most Gang Members Use Social Media, Study Finds*, GOVTECH (Oct. 15, 2013), www.govtech.com/public-safety/Most-Gang-Members-Use-Social-Media-Study-Finds.html.

211. Sara E. Brown, *An Illusory Expectation of Privacy: The ECPA is Insufficient to Provide Meaningful Protection for Advanced Communication Tools,* 114 W. VA. L. REV. 277, 290 (2011) ("Evidence suggests that few users read privacy policies let alone change default settings.").

that being a genetic informant against their distant relatives would be disdainful, the truth is that most people support this use, and some even want to actively participate. When the developers of GEDMatch first heard about the site's role in arresting the Golden State Killer, they expected to quickly hemorrhage users. They certainly did not envision an outpouring of support. However, they received "5,000 new uploads to the site shortly after Mr. DeAngelo's arrest—a daily record."[212] It is clear that not only do the large majority of Americans support FGG, especially when used to solve violent cases,[213] but that banning this methodology would result in far fewer cold cases being solved.

7. Debunking the Claim That FGG Mandates Familial Consent, Where Other Intimate Sharing About Family Members Does Not

Thoughtful scholars writing in this area have suggested that family members ought to get the consent of relatives before uploading their information to sites like GEDMatch.[214] Even some clinical researchers have proposed requiring familial consent, given that hereditary diseases run in families and the information therefore implicates multiple branches in the family tree. Their rationale is that genetic information is unlike other data that we enthusiastically share online because genetic data is immutable, and sharing one's data exposes the data of one's relatives without their consent.

Not so fast. A relative's genotype cannot be neatly predicted for most complex traits, given how random and noisy inheritance can be. This is an important point that needs to be underscored. Having access to my mother's DNA does not tell you whether I am a carrier for any particular disease or whether I will be affected by a genetic mutation. Put more simply, if you knew my mom had the genes for blue eyes, that does not tell you whether I have those same genes, or whether my eyes are, in fact, blue. Since most traits are not autosomal dominant and do not follow simple Mendelian genetics, knowing about someone's SNPs will not tell you much about their cousins' genetic mutations or health risks.

---

212. Murphy, *supra* note 65.

213. Guerrini, *supra* note 8 (Among 1587 respondents, the majority supported police searches of genetic websites that identify genetic relatives (79%) and disclosure of DTC genetic testing consumer information to police (65%). Respondents were much more supportive when the purpose was to identify perpetrators of violent crimes (80%), crimes against children (78%) or missing persons (77%) than when used to apprehend non-violent crimes (39%)).

214. Ram, *supra* note 12; Susan Wallace et al., *Family Tree and Ancestry Inference: Is There a Need for a Generational Consent?*, 16 BMC MED. ETHICS 87 (2015).

Despite these aforementioned caveats, there remains significant concern about the ability of our relatives to spill our collective genetics beans. One of the major critiques of FGG is that your relatives could expose your genetic information or could place you under criminal suspicion through their genealogical research without your consent. But this is fear-mongering.

The "you" in question here is the donor of semen or blood taken from a crime scene or a rape kit. It is the criminal's *own* actions that placed his or her DNA under scrutiny. It may be true that the criminal's name could only be revealed by virtue of his or her relative's contribution to a DTC genetics website. But it was not the GEDMatch user's actions that first placed the suspect under scrutiny. This focuses too much on the reliable identification methodology, rather than the criminal's *actus reus*.

The risk of inadvertent third-party disclosure is much greater with genetically simpler diseases. Knowing that my mother has an autosomal trait tells you quite a bit about me and greatly increases the risk that I will either express or carry the trait. But even then, whether my mother decides to share her genetic disease with others is her choice. While ethically it would be more appropriate for my mother to consult with her close, affected family members before sharing this information with others, it is ultimately her story to tell.

Outside of pedigree and identification, we should be concerned about more nefarious uses by law enforcement or private actors. If the mutations are highly penetrant, quite heritable, and extremely deleterious, we might reasonably be very worried about other people having access to some small and unknown subsect of our genetic information that we never consented to share. Even in these cases, however, analogies to public disclosure of private facts cases suggests that the GEDMatch users would not be liable for uploading their SNP profile to a public site.

c. The Tenancy by the Entirety Analogy Is Not a Good Fit for the Reality of Genetic Information

Legal analysis often turns on which metaphor you select. In a powerful article by Natalie Ram, Ram suggests that we conceive DNA through a property framework, considering the insights provided by the doctrinal metaphor of "tenancy by the entirety."[215] Ram creatively argues that just as tenancy by the entirety forbids one spouse from encumbering shared property without the other

215. Natalie Ram, *DNA by the Entirety*, 115 COLUM. L. REV. 873, 918–19 (2015).

spouse's consent, so too should familial database matching.[216] The government's storage and use of "source-excluding partial matches would encumber the portions of identifiable genetic information shared between known offenders and their close genetic relatives[,]" and thus require the innocent relative's consent.[217] The tenancy by the entirety concept is clever, but it does not track DNA interests very well. For one, we do not "own" our DNA in a technical sense, even though some DTC sites claim that their users own their genomic information. It is not real property, which turns out to matter, as we cannot sell or alter the property rights. More important, however, is the fact that individual DNA mutations do not have much value on their own. With the exception of just a handful of diseases, we must know more about the other protective and deleterious mutations on other alleles in order to process what a particular mutation likely means. We also would need to know more about the individual's diet, history, and life experiences. The property framework overstates our ability to value any isolated piece of DNA.

Also, practically speaking, we are not required to obtain the consent of our family members when we undergo genetic testing or receive test results. These results might implicate a relative's health interests, such as when a mother tests positive for BRCA-1, which marks an increased risk of developing breast or ovarian cancer. For purposes of a tort duty to disclose, courts often expect that if any duty exists, it likely resides with the family member proband, who is expected to communicate these BRCA-1 results to their daughters.[218] Of course, this expectation might be misplaced. But if a duty exists at all, it does not require the proband to keep her information private. Rather, it suggests we might have duties to *disclose* this information to others. This recognizes that privacy interests are different when it comes to genetic risk, which is analogized in these cases to communicable disease.[219]

Further, courts cannot be expected to disentangle the property interests shared even by close relatives like sisters, as they share different percentages of genetics among and between them.

---

216. *Id.* (Familial database searching "constitutes an unlawful effort by the government to encumber not only an offender's interest in her identifiable genetic information, but also the interest of the offender's closest kin.").

217. *Id.* at 920.

218. *See* Safer v. Estate of Pack, 291 N.J. Super. 619, 625 (N.J. Super. Court. App. Div. 1996). For a general discussion of the tort duties to warn family members of genetic risk, *see* Teneille R. Brown, *Needles, Haystacks and Next-Generation Genetic Sequencing*, 28 HEALTH MATRIX 217, 263 (2018).

219. *Safer*, 291 N.J. Super. at 625 ("There is no essential difference between the type of genetic threat at issue here and the menace of infection, contagion or a threat of physical harm.").

This would become even more unwieldy if we were instead discussing property rights in shared regions of homozygosity hovering around 1-2% of the genome, which would vary from one cousin to another.[220] Would the property right be determined at the level of the SNP, or at the level of the collective, polygenic risk? Or only for SNPs that predict clinically actionable traits? The fact that we still do not know much about the connection between genotypes and phenotypes suggests that a property framework will not work. Finally, because our genetic information is increasingly being used for precision medicine, these applications implicate autonomy and substantive due process much more than encumbrances on shared real estate.[221] Substantive due process rights under the Fourteenth Amendment would likely prevent governments from requiring the permission of each sibling before making autonomous, individualized health care decisions.[222] While it might be ethically appropriate for probands to discuss their genetic test results with family members and request permission from them before sharing those results with others, their results are currently their own.

Rather than analogizing DNA to property, an analogy to non-genetic information seems to make more sense. After all, what is concerning to privacy scholars is the use of this DNA to make interpretations, however shaky, about someone's ancestry, identity, or health risks. It is not the DNA, *qua* DNA, that is protected. It is the translation from DNA mutations to our health and identity that contains informational value.[223] Thus, metaphors sounding in disclosure of information, rather than encumbrance of property, are probably more useful for thinking about the legal implications of sharing genetic data.

---

220. *But see* Ram, *supra* note 12 ("[C]ourts should look to other forms of shared material to illuminate analysis about when an individual has a sufficient interest in searched genetic data that does not derive from their own cells.").

221. Alessandro Blasimme & Effy Vayena, *Becoming Partners, Retaining Autonomy: Ethical Considerations on the Development of Precision Medicine*, 17 BMC MED. ETHICS 67 (2016).

222. Cruzan v. Dir., Mo. Dep't of Health, 497 U.S. 261, 265, 110 S. Ct. 2841, 2844 (1990). ("No right is held more sacred, or is more carefully guarded, by the common law, than the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law. This notion of bodily integrity has been embodied in the requirement that informed consent is generally required for medical treatment.").

223. Julyan Cartright et al., *DNA As Information: At the Crossroads Between Biology, Mathematics, Physics and Chemistry*, 374 PHIL. TRANS R. SOC. 20150071, *7 (2015) ("The genetic code is not a book nor part of it; rather, it is a translation dictionary between two different worlds (languages), i.e., the world of nucleic acids and the world of proteins . . . Moreover, little is known about the grammar, the syntax, and even the orthography of the book of life.").

d. The Metaphor of Memoir Provides a Much More Useful Framework for Analyzing Genetic Privacy in This Domain

Autobiography provides a very useful, if imperfect, metaphor for the sharing of our genetic information with others. Just as the memoirist reveals information that is mostly "her story," she is also telling part of the private stories of others, who never consented to this story being told. Further, just as with autobiography, the genetic story told by the author is colored by each sibling's unique contribution and idiosyncratic perspective.[224] If an account or memory is disputed, it is difficult for the reader to unravel the different threads to determine which part of the story is true and whether the sources are reliable. One First Amendment scholar argues this gives memoirs greater, rather than less, narrative power.[225]

This sort of imperfect accounting is also true for the information shared in our genomes. Even close relatives like siblings have very different genomes, or genetic stories, that cannot be surmised from our own. Furthermore, it can be difficult to determine what we share versus what is unique. Even still, outside readers might draw inferences about a heritable trait and presume that we are carriers until proven otherwise, so we might expect family members to keep this sort of information private. Finally, just like with genetics, our family story is what it is, and it cannot be changed. Of course, we can reinterpret our history and memories, but the facts that underlie them exist in the past and are immutable. Once someone knows about a private aspect of our past, such as our parents abusing drugs or that we were conceived through rape, we cannot change these facts, just as we cannot presently change our autosomal genes.

There is a flourishing memoir ethics literature that discusses how authors ought to tell their stories, knowing that in so doing they are divulging others' secrets.[226] F. Scott Fitzgerald's *Tender is the Night* is a gut-wrenching autobiographical account of his wife's sad descent

---

224. *See* Sonja R. West, *The Story of Me: The Underprotection of Autobiographical Speech*, 84 WASH. U.L. REV. 905, 933 (2006).

"This ambiguity over the truth or falsity of memories is even more pronounced when the stories involve not just provable facts but human relationships, emotions, or reactions…[t]hus, there might be argument that there is something uniquely valuable about individual memories, perceptions, and viewpoints on personal life events regardless of their verifiable accuracy. Under this view, autobiographical speech might be deserving of protection beyond the boundaries of basic defamation law."

225. *Id.*

226. Carolyn Ellis, *Telling Secrets, Revealing Lives*, 13 QUALITATIVE INQUIRY 3, 14 (2007).

into madness. While many readers appreciated the honesty of the story, some questioned Fitzgerald's "right to violate Zelda's privacy, with no realistic opportunity either for consent or for telling her story her own way."[227] In the present context of genetics, researcher and author Alex Wexler wrote a loving memoir about her mother's Huntington's disease and her own research to help discover its genetic causes.[228] Recognizing the moral complexity of her memoir, Wexler grappled with the "potentially severe consequences [of her disclosures] for people she cares about."[229]

There are certainly ethical quandaries authors face when choosing to tell their stories that implicate the stories of their parents and siblings. Sometimes auto-biographies include intensely personal accounts of rape,[230] addiction,[231] or incest[232] that occurred in the family home, which other family members would rather keep private. But even in these cases where the shared content is deeply sensitive and potentially embarrassing, the courts have almost always sided with the authors.[233] The individual's First Amendment right to "tell her story" usually trumps the family member's expectation of privacy. This is true even when the subject whose

---

227. Martha Montello, *Confessions and Transgressions: Ethics and Life Writing*, 36 HASTINGS CENT. REP. 46, 46 (2006).

228. Alex Wexler, *Mapping Fate: A Memoir of Family, Risk, and Genetic Research*, U. CAL. PRESS (1996).

229. Montello, *supra* note 227.

230. "The Court must believe that the First Amendment greatly circumscribes the right even of a private figure to obtain damages for the publication of newsworthy facts about him, even when they are facts of a kind that people want very much to conceal." Haynes v. Alfred A. Knopf, Inc., 8 F.3d 1222, 1232 (7th Cir. 1993) (discussing a rape victim being identified in a book as being unable to bring a public disclosure of private facts claim against the publisher).

231. "This is my story…It's not my mother's story and it's not the family's story, and they may remember things differently and they may choose to not remember certain things, but I will never forget what happened to me, ever, and I have the scars from it and I wanted to rip those scars off of me." Buzz Bissinger, *Ruthless with Scissors*, VANITY FAIR, Jan. 2007, at 104, 108 (quoting author of *Running with Scissors*, Augusten Burroughs, describing why he wrote the piece).

232. Anonsen v. Donahue, 857 S.W.2d 700, 705 (Tex. App. 1993), *cert. denied*, 511 U.S. 1128 (1994).

233. "[T]here is an additional interest in this case: Kaysen's right to disclose her own intimate affairs. In this case, it is critical that Kaysen was not a disinterested third party telling Bonome's personal story in order to develop the themes in her book. Rather, she is telling *her own* personal story-which inextricably involves Bonome in an intimate way. In this regard, several courts have held that where an autobiographical account related to a matter of legitimate public interest reveals private information concerning a third party, the disclosure is protected so long as there is a sufficient nexus between those private details and the issue of public concern." Bonome v. Kaysen, No. 032767, 2004 WL 1194731, at *6 (Mass. Super. Ct. Mar. 3, 2004).

private information is being revealed had no part in the construction of the memoir.[234] One court went even further, suggesting that whether or not the underlying material is newsworthy is irrelevant to whether the author has the right to reveal "her own identity."[235] It is presumed that she possesses this right, even if exercising it means revealing private information about those close to her.

These cases are instructive as applied to our genomic information. When I choose to obtain genetic tests to complete my genetic story, either to assist in precision genetics treatments or to connect with distant relatives, I am writing *my* story. I am gathering information and sharing it because it is my autonomous choice. This decision might indirectly implicate the privacy of others, and it might hurt them. Consider for example, a family who identifies as Native American only to discover through genetic ancestry testing, that there is no evidence, at least according to Ancestry's algorithm, that this family folklore is true. Do I have a privacy interest in my family's ancestry story? Perhaps. Will the law recognize this and protect it from disclosure by a family member? No. Just as with memoir, where "it is often difficult, if not impossible, to separate one's intimate and personal experiences from the people with whom those experiences are shared," it is likewise difficult to separate out which traits or SNPs run in your family, what those SNPs predict in isolation and in your particular pedigree, and what that shared genetic information reveals about any one person.[236] Put differently, Alex Wexler can certainly publish her story about her family's experience with Huntington's disease without being liable for an invasion of privacy claim. The case law is clear on this point. However, we are dealing with an even more amorphous kind of privacy threat. When my genetic story becomes even less concrete, and involves describing *potential* genetic risks rather than actual disease symptoms, the right to privacy for my relatives becomes even weaker.

Of course, one could argue that when police surreptitiously submit crime-scene DNA samples, they are forcing someone else to "tell their story" and connect with family members against their wishes. In one sense, this is true. But once again, given that the DNA is significant evidence of having committed a criminal *actus reus*, the

---

234. There is a First Amendment privilege to publish truthful information of legitimate public concern, and the privilege encompasses dissemination of information relating even to individuals who have not sought or who have attempted to avoid publicity. *See* Campbell v. Seabury Press, 614 F.2d 395, 397 (5th Cir. 1980).

235. *Anonsen*, 857 S.W.2d at 705.

236. *Bonome*, 2004 WL 1194731, at *6.

privacy rights in that DNA are substantially diminished.[237] It hardly seems controversial ethically, and is certainly true legally, that a criminal has relinquished the right to tell his own story with his DNA. The law is utilitarian when it comes to privacy, not absolute. Because the purpose was to identify a murderer, the public certainly has an interest in the disclosure of the crime-scene DNA to GEDMatch to find a relative, if not in knowing its specific content.[238]

In conclusion, existing law would not require anything like familial consent before law enforcement could use FGG. Genomes are individually unique constructions, and the value of an entirely different genome, with a different combination of mutations and life experiences, cannot meaningfully be compared through the tenancy by the entirety metaphor. Assuming that our genes have independent property value, without any accompanying information about environmental risk or the interactive effects of our genes, relies on genetic determinism, wherein we assume we can know someone from their genes alone.[239]

Despite its allure, the property metaphor (which I assume is not meant to be literally implemented) just does not work well in the context of sensitive and highly idiosyncratic DNA information. Specifically, alienation, valuation, transfer, license, sale, etc., would be unwieldy. Not only does the case law make clear that family members can reveal photographs and private, scandalous family histories, but it really must be this way.

If family members were required to obtain the consent of their relatives before obtaining genetic test results or sharing them, would that extend only to immediate family members, or to anyone with shared DNA, including some holdout who could be a fourth cousin? Could a fourth cousin keep me from sharing my BRCA-1 results with my granddaughters? Given that most people do not consider their fourth cousins to be within the boundary of their "family," and given that without a service like Ancestry they would likely not even know who these fourth cousins were, it is a bit preposterous to suggest that their consent would be legally (as opposed to ethically) required *ex ante.*

---

237. Hodge, *supra* note 146.

238. "[A]n involuntary loss of privacy is recognized in the modern formulations of this branch of the privacy tort, which require not only that the private facts publicized be such as would make a reasonable person deeply offended by such publicity but also that they be facts in which the public has no legitimate interest." Haynes v. Alfred A. Knopf, Inc., 8 F.3d 1222, 1232 (7th Cir. 1993).

239. This concept will be discussed in more detail in Section H.

Most importantly, in the context of precision medicine, it would be appalling to require an individual to receive her siblings' consent before undergoing genetic testing. Even without genetic testing, information about particular diseases (such as breast cancer, or depression) is already known to run in families. Family members often know their history; the genetic information may just confirm whether they are a carrier or at risk, but it's not a surprise that this risk is familial. Given the way this risk data is understood and communicated, an approach that treats it like information is far preferable.

G. Why Do Scholars Fear Genetic Informants?

1. Our Fear of Genetic Informants Reflects Moral Dumbfounding

As explained in the sections above, very few of the privacy concerns surrounding FGG stand up to scrutiny. In many cases, the arguments against FGG illustrate a form of "moral dumbfounding,"[240] where opponents find the method morally questionable but cannot locate a good argument as to why. Jonathan Haidt described this phenomenon as thinking like a "lawyer trying to build a case rather than a judge searching for the truth."[241] Moral dumbfounding leads to weak rationalizations for things that seem intuitively immoral (and may indeed *be* immoral, but for reasons we cannot articulate).

In some cases, critiques of FGG, based on an intuitive sense that it is immoral, have worked. Legislators in Maryland proposed bans on this useful prosecutorial tool because of inflated privacy concerns. These concerns reflect a misunderstanding of criminal procedure and of the *status quo ante*. The fact that such bright legal minds can be so confused about the actual privacy implications of FGG intimates that there is something deeper at work. This is more than just a failure to analyze case law precedent on the Fourth Amendment, witness testimony, the police use of deception, or the invasion of privacy.

2. Our Fear of Genetic Informants Reflects Genetic Essentialism

---

240. Jonathan Haidt et al., *Moral Dumbfounding: When Intuition Finds No Reason*, in 1 No. 2 LUND PSYCH. REP. 1, 1–29 (Dep't of Psychology, Lund Univ. ed., 2000).

241. Joshua May & Victor Kumar, *Moral Reasoning and Emotion*, in THE ROUTLEDGE HANDBOOK OF MORAL EPISTEMOLOGY 139, 142 (Karen Jones et al. eds., 2019).

The reason, I suggest, that leads to these fears is subconscious endorsement of genetic essentialism. First, essentialist thinking leads people to believe that genetic explanations are truly exceptional. Therefore, relevant precedent is immediately and always distinguishable. Second, it leads people to believe that genes are more deterministic than they actually are. This in turn encourages an overemphasis of genetic causes of behavior over environmental factors and a need to protect these immutable blueprints from disclosure. Third, when people think about genes in essentialist ways, they may adopt genetic vitalism, where an almost mythic agency or intentionality is attributed to our genes. Vitalism may explain the view that FGG is "dystopian" or "creepy," as we consider our genes to be unintentional informants. This might explain why some fail to disambiguate the inanimate DNA from the individuals' actions, which allowed others to access the DNA.

Essentialist thinking has been demonstrated in many different cultures and contexts. We all engage in it to a degree. However, some people are more essentialist than others, and some topics, such as genetics, tribalism, or race, lead people to engage in more rigidly essentialist thinking. Essentialists find greater causal power in people's fixed characters than in their surroundings, and assume that much of one's behavior can be explained with reference to the essence that they have.[242] This sort of thinking is on display when we think that something represents "who we truly are," in a way that is "deep down and internal," "naturally determined," which "draws the boundaries" between social groups, and can be "transferred from individual to individual while preserving their original identity."[243] Natural things have an essence; synthetic things do not. In this way, essences are often conceived of as something like a soul, like *chi* in Chinese cultures or *prana* among Hindus.[244] Given these chief features, it is no wonder that genetics so handily lends itself to essentialism.

It seems some of the critiques of FGG sound in the type of genetic essentialism that treats genetics as completely exceptional. This might explain why scholars have failed to properly consider precedent regarding privacy and criminal procedure. They may assume that our genomes cannot be properly analogized to *anything that has come before*. In some ways, our genomes are special and present novel concerns about privacy. Namely, while we might disclose our genomes today, the predictive power of our genomes will continue

---

242. Steven Heine et al., *Essentially Biased: Why People are Fatalistic About Genes*, 55 ADVANCES IN EXPERIMENTAL SOC. PSYCHOL. 137, 142 (2017).

243. *Id.*

244. *Id.* at 148.

to grow. Ten years from now, we will likely know even more about disease risk and penetrance than we do now, and that makes sharing genetic data related to disease risk very different. However, when SNP data are used to identify relatives, it is not taking on a form that is radically different from public archives, peer-to-peer sharing of pornographic files, or searching of social media posts. When it comes to the ways genetics is being used in the service of FGG, there are no sufficiently strong reasons to justify its exceptional treatment.

Genetic essentialism leads people to do a number of strange things. For one, they will "over-attribute a person's characteristics and behaviours, in all of their complexity, to their genetic makeup,"[245] and they will tend to view genetic risk factors as being more causal, or deterministic of outcomes, than they actually are.[246] This has the related effect of discounting other causes of disease, behavior, or identity, such as culture, diet, or the environment.[247] There are a handful of diseases wherein genes operate in hard, deterministic ways, and for which you could actually have "a gene for" the disorder that means you will definitely develop that condition. These Mendelian traits are actually pretty rare. Even so, "people overgeneralize from these to the far more common conditions where genes are not at all deterministic."[248]

Genetic determinism might move us to accord genes more heightened privacy protections than are warranted for their specific use. In the deterministic view, genes are perceived to so completely control our future that this justifies our need to keep them secret. I strongly suspect that some of the "moral dumbfounding" surrounding FGG has to do with precisely this. We worry about people having access to genetic information because we assume that there is a one-to-one relationship between genotype and phenotype, and that if we have a mutation that increases the risk of depression or addiction, we will certainly develop depression and addiction.[249] This makes genetic information much more sensitive, as it is perceived to provide a crystal ball for our future.

---

245. Ilan Dar-Nimrod et al., *Genetic Knowledge Within a National Australian Sample: Comparisons with Other Diverse Populations*, 21 PUB. HEALTH GENOMICS 133, 134 (2019).

246. Wren Gould & Steven Heine, *Implicit Essentialism: Genetic Concepts Are Implicitly Associated With Fate Concepts*, PLOS ONE, June 2012, at 1.

247. Ilan Dar-Nimrod & Steven J. Heine, *Genetic Essentialism: On the Deceptive Determinism of DNA*, 137 PSYCHOL. BULL. 800, 800 (2011).

248. Heine, *supra* note 242, at 150.

249. *Id.*; *see also* Mark Henderson, *'Fat' Gene Found by Scientists,* THE TIMES (U.K) Apr. 13, 2007, www.thetimes.co.uk/article/fat-gene-found-by-scientists-vbf7scwhhnn.

In reality, the SNPs that are used to make disease predictions explain very little of the variance between individuals, so this data is currently of limited individual predictive value.[250] Most complex diseases are caused by many different mutations that interact with one another in as-yet-unknown ways. DTC results also fail to capture varying genetic expression, which is affected by lifestyle choices and environmental risks.[251] However, for some diseases, such as Alzheimer's, the identified variants are linked to a substantial increase in the risk of developing that disease, and they are thus more clinically useful. In the future, DTC companies might rely on sequencing the entire genome, which would provide vastly more information on rare diseases than that which is gleaned from just SNPs alone. The potential for using genetics in increasingly predictive ways means we should be mindful of the privacy and security of our genetic data. But this sort of prediction is not inherently at stake with FGG.

Long before we knew about the structure of the double helix, biologists debated whether biology could be explained solely by the principles of physics and chemistry.[252] Many eighteenth and nineteenth century biologists theorized that biology contained metaphysical and spiritual properties, which might never be knowable through the laws of the hard sciences. This came to be known as "vitalism," where biological processes were imbued with agency, desires, and ultimate goals.[253] Vitalism is now largely discredited and dismissed as superstitious.[254] Even so, vitalism is alive and well in our folk understandings of biology. Without being able to prove this directly, I suspect that some of our suspicions of the "genetic informant" or the "biowitness" have to do with our subtle and subconscious misattribution of agency and intent to our genes.

Anthropomorphism is a "false positive bias" where we over-attribute human-like characteristics such as agency, intention, purpose, or volition, to objects that possess no such capacities.[255] It can happen with inanimate objects, as well as with non-sentient organisms. Even if it is incorrect, it is the result of an over-active and fascinatingly adaptive cognitive process.[256] Because the

250. Park et al., *supra* note 27.

251. Bunnik et al., *supra* note 43, at 344.

252. Marc Kirschner et al., *Molecular Vitalism*, 100 CELL 79, 79 (2000).

253. Monica Greco, *On the Vitality of Vitalism*, 22 THEORY, CULTURE & SOC'Y 15, 16 (2005).

254. *Id.* at 15.

255. Marco Antonio Correa Varella, *The Biology and Evolution of the Three Psychological Tendencies to Anthropomorphize Biology and Evolution*, FRONTIERS IN PSYCHOL., Oct. 2018, at 1.

256. *Id.* at 10.

anthropomorphism tendency is so pervasive, involuntary, and deeply-rooted, it is studied in many different disciplines. Within cognitive psychology, it is called "teleological obsession" or "overactive intentionality bias," and is employed to explain why people presume intentionality where there is no evidence of its presence.[257] Within psychiatry, it is known as "hyper-mentalizing" where it sheds light on why people with schizophrenia or other mental illnesses might imbue mailboxes and computers with secret intentions and surveillance capacities.[258] As applied to biological processes, this tendency is often referred to as vitalism.[259] Regardless of what you call it, there is consensus that anthropomorphism is expressed at such a young age, and is so powerful and automatic, that it feels (and may indeed be) innately hardwired.[260] We can therefore be forgiven for engaging in the particular form of anthropomorphism that implicitly recognizes intentional action in our genes.

If one thinks of FGG as employing DNA as "genetic informants" or "biological witnesses,"[261] it calls to mind something out of a dystopian science fiction novel. The use of these anthropomorphizing labels suggests that it is in fact the *DNA itself* that is testifying against you. This is of course deeply unnerving, in part because of humanity's inherent desire to control its environments. If an independent and intentional genetic informant can speak for us in this way, this reveals something profoundly scary—that we humans are not fully in control of our actions or their consequences. This is particularly troubling when the consequences seem so great. Rather than being able to decide whether to implicate our relatives in a crime, our genes are seemingly making this decision for us, without our consent. I suspect that this phenomenon is also at the root of our response to FGG.

Viewing FGG as employing "genetic informants," as many of its opponents do, exploits the psychological fear of losing control of our environment and our free will.[262] Humans have a strong desire to "master their environments by increasing the environment's predictability" through its "apparent controllability."[263] Put simply, if we are not controlling our genes, we fear that they are controlling us. The need to feel in control of our environments is referred to as "effectance motivation," and is a

257. Varella, *supra* note 255, at 1–4.
258. *Id.* at 1, 2.
259. Kirschner et al., *supra* note 252.
260. Varella, *supra* note 255.
261. Kayser, *supra* note 165, at 45.
262. Nicholas Epley et al., *On Seeing Human: A Three-Factor Theory of Anthropomorphism*, 114 PSYCHOL. REV. 864, 872 (2007).
263. *Id.*

big driver of anthropomorphism.[264] Attributing human-like properties to biological entities enables a sense of familiarity and, therefore, control over them.[265] This in turn provides a feeling of comfort when interacting with these agents.[266] Ironically, we employ anthropomorphisms to make us less afraid of losing control. However, because our brains evolved to over-apply it in novel contexts, it can actually make us more afraid of unintentional agents, like robots or genes.[267]

Of course, our genes are not intentionally testifying against us. But given the pervasiveness of anthropomorphizing, especially toward a biological phenomenon like genes, it would not be at all surprising if this causes our strong negative reaction to FGG. The language of the "genetic informant" or "biowitness" unnecessarily imbues the DNA with properties that it does not possess. For our purposes, these terms are misleading because they obfuscate the intentional actions of ordinary people.

III. CONCLUSION: REFORMS THAT BETTER ADDRESS THE REAL PRIVACY CONCERNS OF FGG, WITHOUT HAMPERING THE PROSECUTION OF SERIOUS CRIMES

Secondary use of genetic information by private actors without consent should certainly give us pause. And the unlimited potential uses by the government should also generate considerable worry. But by focusing on the Fourth Amendment concerns of FGG when it is used exclusively by law enforcement to identify the perpetrators of crime, privacy advocates emphasize the wrong privacy boogeymen and thus propose the wrong remedy. We should not ban FGG when used to identify suspects in cold cases. We might, however, decide that DTC genetic companies, while technically consumer enterprises, might share enough features with clinical care to legally require additional consent measures before people participate. We might also limit the secondary uses of DTC genetic information in some meaningful ways. I briefly sketch out the justifications for these very different reforms below.

a. Statutory Secondary Use Restrictions

I suspect it would be different if, rather than using regions of homozygosity and ancestry information, law enforcement

264. Adam Waytz et al., Making Sense by Making Sentient: Effectance Motivation Increases Anthropomorphism, 99 J. PERSONALITY & SOC. PSYCHOL. 410, 410 (2010).

265. *Id.*

266. *Id.* at 879.

267. *Id.* at 872.

connected the family through a rare and serious disease mutation that ran through the family, and was evidenced in health records or a SNP profile. If law enforcement identified and publicized that the GEDMatch user was affected, this would likely run afoul of legally recognized privacy rights. But even if this *had* been the case, there is no indication that law enforcement would ever need to reveal the rare mutation discovery to the GEDMatch user, just as they never identified Joseph DeAngelo's distant relative who provided the genetic connection that led to his arrest.

The possibility that law enforcement, or other commercial entities, could glean clinically relevant information from GEDMatch profiles is troubling. And yet, because users voluntarily uploaded their SNP data to an open-access, amateur genealogical website, they have no recourse under existing law, at least against secondary data users.[268] In order to better address this sort of harm, we must educate consumers more about the vast amounts of data they are sharing with sites like GEDMatch, or even 23andMe and Ancestry. There also should be significant secondary use limitations that delineate how law enforcement may and may not use the genetic profiles that they, and other private actors, have obtained. Perhaps we need a federal statute that allows law enforcement or private entities to use these SNP profiles only to identify perpetrators after they have committed crimes, to identify the remains of bodies, or to reunite displaced persons or victims of human trafficking with their families. There could conceivably be limitations on the types of crimes for which it could be used, based on political sentiment.

As far as we know, law enforcement has not yet used SNP data to do anything other than identify suspects of serious crimes. If we fear that law enforcement could use this data to predict health traits or conduct internal research, then the solution is not to ban

---

268. The relatives of the family member (proband) who uploaded her data to GEDMatch may theoretically have a right of action in tort law against the proband. For example, if I upload my SNP profile to GEDMatch, or some other third-party site with insufficient privacy protection by design, my daughter might be able to sue me for public disclosure of private facts, if the state court were willing to find that this sort of disclosure was embarrassing, unreasonable, and at least reckless. However, this might not be recognized, depending on how strong the public interest is in the disclosed information. *See* Cox Broadcasting Corp. v. Cohn, 420 U.S. 469, 487–91 (1975); Time, Inc. v. Hill, 385 U.S. 374, 383 n.7 (1967); *see also* Virgil v. Time, Inc., 527 F.2d 1122, 1127 (9th Cir.1975). The purpose of the tort remedy is to protect the individual against unwarranted publication of private facts. The individual's right to privacy must be balanced with the privilege of the press to publicize matters of public interest that arise out of the desire and "the right of the public to know what is going on in the world and the freedom of the press and other information agencies to report it." *See generally* RESTATEMENT (SECOND) OF TORTS § 652 (1979).

FGG. It is not just the police who have access to this rich SNP data. *Anyone* who has access to SNP profiles could upload genetic SNP data to a public site and search for the sample's relatives. This is because GEDMatch and FamilyTreeDNA do not require any identity authentication.

Rather than banning FGG, the solution to this sort of problem is to craft thoughtful legislation that limits certain secondary uses of DTC genetic information. Obvious candidates would be prohibiting the use of SNP data to price health, life or disability insurance, or increasing the fines associated with detection of these uses. Unfortunately, the federal statute prohibiting the use of genetic information to make health insurance coverage or employment decisions might not account for low detection rates, and the scope of GINA's broad exceptions have been insufficiently fleshed out.[269] Another candidate would be requiring specific consent to use samples in research. A large part of 23andMe's business model rests on the secondary use of genetic samples for health research. By sharing SNP data with outside researchers, promising research is being pursued that will help us treat cancer or heart disease more effectively. Not all secondary uses are sinister. But we might reconsider the model where simple disclosure of many terms and acceptance by consumers is considered legally sufficient.

b. Mandatory Updates of the Consent Process for DTC Genetic Tests

Multiple reviews of the consent process for DTC genetic testing reveal that the user agreements and consent procedures are wholly inadequate, especially given that no physician is made available to explain the risks and benefits.[270] There is a reason that countries like France, Germany, Luxembourg, Poland, and Portugal demand that physicians be involved in the ordering of any genetic test.[271] Regulators in those countries appreciate the enormous risks posed by the inappropriate delivery and interpretation of this sort of information. Consumers of DTC genetic tests may not understand how to interpret the various findings. There are mutations associated with tiny relative risk increases, mutations with unknown expression or population penetrance (because many DTC tests are

269. Bradley A. Areheart & Jessica L. Roberts, *GINA, Big Data, and the Future of Employee Privacy*, 128 YALE L.J. 710, 728 (2019). For example, employers can use genetic information that they obtain inadvertently or via commercially available documents, like newspapers that contain obituaries.

270. Clayton et al., *supra* note 14.

271. Louiza Kalokairinou et al., *Legislation of Direct-to-Consumer Genetic Testing in Europe: A Fragmented Regulatory Landscape*, 9 J. COMMUNITY GENETICS 117, 123 (2018).

run in asymptomatic individuals, the likelihood of someone developing the disease associated with a mutation is unknown), or mutations of unknown significance. Further, DTC tests have varying levels of laboratory and clinical quality. Some are not reliable, meaning that many runs of the test will produce varying results, and some are not valid, meaning that the results do not mean what we think they do. We also might worry about this sort of sensitive information being relayed without the possibility of counseling to put the findings in context. For these reasons and others, many countries require that genetic susceptibility tests only be performed as part of clinical care. These countries therefore require physician involvement and patient-informed consent.[272]

A recent review of European regulations found that fourteen countries had specific requirements for informed consent for DTC genetic testing. Some of these countries require meaningful disclosure of all relevant risks and benefits, a right "not to know" the information should they change their mind before the results are delivered, and appropriate time be given before the test and after disclosure for the individual to consider consenting.[273] There is considerable variation among countries regarding which DTC genetic tests require informed consent, what must be present in the consenting process, and the consequences of non-compliance. In Germany, for example, failing to provide advance, express written consent is punishable by imprisonment or a fine. [274]

Regrettably, the United States has not taken this approach. Instead, in the U.S., DTC genetic testing operates largely outside of the realm of "health care," despite interacting with it in many ways. Consumers who undergo testing may become patients who seek physicians' help confirming or interpreting the results. They also may use the testing to decide whether to have a preventative procedure like a hysterectomy or whether to become involved in clinical research. Another large number of them may never use the data in an officially clinical way, but it might subtly change the way they think about their health, and for-profit entities might exploit their data in ways that affect the individual's access to care in the future. Even so, DTC testing in the U.S. is considered mostly recreational. Thus, testing generally does not require physician involvement or clinical informed consent. This is the root of the problem. Despite perhaps being ethically required, outside the

272. *Id.*
273. *Id.*
274. *Id.* at 124.

context of clinical care and research, the requirement for informed consent is not widely recognized.[275]

As a result, a few different research teams have documented the consent processes for DTC consumer tests and found them troublingly flawed. Indeed, the use of the phrase "consent processes" is misleading, as most DTC genetic testing companies just employ user agreements that consumers must click on in order to use the services or website. Third-party sites like GEDMatch have been found to have particularly poor procedures for documenting agreement with the terms of service.[276] For most DTC genetic tests, users find privacy protections important and desire control over the dissemination of their genetic information. However, they mistakenly assume that the DTC genetic companies are fully protecting their privacy rather than sharing their data with third-party researchers.[277] A study of DTC genetic testing companies targeting Canadian consumers found that "67% provided information insufficient for consumers to determine how their data and sample would be treated."[278] This is alarming, and certainly indicates that a significant part of our trouble with FGG might stem from concerns over meaningless consent at initial stages of testing.

Although more companies now meet guidelines relating to transparency regarding data security protocols, few companies disclose which secondary uses of users' data would be permitted, with whom they would contract, how long the information would be stored, and what might happen in the event that the company was sold or went bankrupt. This finding was supported by smaller, more in-depth studies, which revealed failures to convey the risks of re-identification and to obtain proper consent for the secondary use of data.[279] The privacy and security risks are critically important, given

---

275. Bunnik et al., *supra* note 43, at 343.

276. Lauren Badalato et al., *Third Party Interpretation of Raw Genetic Data: An Ethical Exploration*, 25 EUR. J. HUMAN GENETICS 1189, 1190 (2017).

277. Clayton et al., *supra* note 14; Juli Murphy Bollinger et al., *Attitudes About Regulation Among Direct-to-Consumer Genetic Testing Customers*, 17 GENETIC TESTING AND MOLECULAR BIOMARKERS 424, 424-28 (2013); Saskia Sanderson et al., *Public Attitudes Toward Consent and Data Sharing in Biobank Research: A Large Multi-site Experimental Survey in the US*, 100 AM. J. HUMAN GENETICS 414, 414–27 (2017); Sara Chandros Hull et al., *Patients' Views on Identifiability of Samples and Informed Consent for Genetic Research*, 8 AM. J. BIOETHICS 62, 66 (2008).

278. Amanda Singleton et al., *Informed Choice in Direct-to-Consumer Genetic Testing (DTCGT) Websites: A Content Analysis of Benefits, Risks, and Limitations*, 21 J. GENETIC COUNSELING 433, 433 (2012).

279. Linnea I. Laestadius et al., *All Your Data (Effectively) Belong to Us: Data Practices Among Direct-to-Consumer Genetic Testing Firms*, 19 GENETICS IN MED. 513, 513 (2017); Emilia Niemiec & Heidi Carmen Howard, *Ethical Issues in Consumer Genome Sequencing: Use of Consumers' Samples and Data*, 8 APPLIED TRANSLATIONAL GENOMICS 23 (2016).

the market value for this sort of data and the temptation for unsavory companies to hack into databases to glean genetic and phenotypic information for research.[280] Unfortunately, these concerns have only been amplified with the increasing use of more modern and thorough genetic sequencing technologies.[281]

It is not uncommon for commercial entities to exploit the appearance of being "medical" to confuse consumers into thinking the experience has the legitimacy and scientific backing of the healthcare system. Based on a review of their advertising practices, many DTC genetic testing companies seem to do exactly this.[282] Several were found to exploit the professional legitimacy of a clinical encounter to establish trust between the company and the consumer, while in their small print user agreement they disavowed many of the regulatory protections that come with clinical experiences such as informed consent, HIPAA compliance, and notification and opportunity to withdraw data if the user no longer wishes to participate in the research database.[283] Clinical care obviously differs considerably from consumer advertising, both in its ethical and legal requirements. It is important for consumers to know what they are buying and sharing.

Medical ethics requires that clinicians respect the autonomy of their patients by disclosing all relevant risks and benefits of a procedure or test *before* it is performed. This has become so standard that the law of every state now requires informed consent in order for physicians to be free from either negligence or battery liability. More modern takes on informed consent stress that disclosure, wherein the clinician provides information in written form and obtains a signature by the patient, should not be a mere formality. Rather, to affect meaningful informed consent, patients ought to be able to understand enough of the procedure to ask questions and have time to reflect before making a decision. They also ought to be given the opportunity to change their consent status, when possible.

However, none of these legal or ethical standards have been found to apply to DTC companies because they are regulated as if they provide a purely commercial service. This is a mistake. It may be that part of the reaction to FGG lies in consumer discomfort with law enforcement having access to our genetic information, or a misunderstanding of who has access to this complex information in

280. Laestadius et al., *supra* note 279; Niemiec & Howard, *supra* note 279.

281. Niemiec & Howard, *supra* note 279.

282. Manuel Schaper & Silke Schicktanz, *Medicine, Market and Communication: Ethical Considerations in Regard to Persuasive Communication in Direct-to-Consumer Genetic Testing Services*, 19 BMC MED. ETHICS 56 (2018).

283. *Id.*

the first place. This suggests our consent process is not working, and for this and other reasons, it might be unwise to allow consumers to be tested "recreationally" for genetic mutations that carry potential for significant future non-recreational uses.

Because genetic information is so complicated, it is not possible to provide all the relevant risk and benefit information in one setting, particularly if done online. Informed consent for DTC testing ought to include an initial layer of basic information on how the saliva sample will be obtained, the laboratory procedures, and what tests may be run on that sample.[284] Customers should also be told about the risks of false positives, false negatives, and laboratory errors. If consumers affirmatively click to agree to these conditions, then a second layer of information should convey background knowledge on genetic expression and penetrance. This layer should include videos and images to simplify the complex information and identify and use some traits with high and low penetrance and expression as examples. Consumers should then be given notice on what others with this data can do with this information. This layer should include information about GINA, and what it protects. It can also describe how our genetic information does not change over the course of our lifetime and how this information could be used to identify us or others through methods like FGG. Again, the use of interactive videos might be useful to help illustrate the data behind these processes.

Next, if someone is interested in pursuing genetic information about health risks, there ought to be *another* layer of consent where consumers are briefed on the different kinds of health risk data. Specifically, consumers should have to opt-in to receive carrier or susceptibility information regarding penetrant health traits, particularly for which there are no known treatments or for which there is a significant and negative prognosis for either themselves or their offspring. Examples of this would include disclosing risks of Huntington's disease or Alzheimer's disease.[285] It is shocking that companies are not required to run these tests through a medical provider, given the potential psychological impacts of the results.

Some consumers may altruistically wish to contribute their genetic information to a database used for research purposes. If consumers agree to participate in a commercial research database managed by the DTC company, and have their samples or personal information used by research teams, then another layer must explain

284. Bunnik et al., *supra* note 43.
285. Bunnik et al., *supra* note 43, at 345.

this process in detail. Consumers must be told what types of research might be conducted, what personal information of theirs will be used, how they might be later identified using this data, and with whom the data might be shared. Because genetic information—even when stripped of our names, birthdates, addresses, and other readily identifiable information—still has the potential to identify us and is immutable, consumers should have the opportunity to stop participation in this research at any time. Of course, this cannot undo the research and data sharing that has already occurred, but it is important in the event that a research company is sold to a less reputable company that one may then change the user agreement and protections.

Third-party sites like GEDMatch should also require a more robust consent procedure. If the sites are not conducting the tests themselves, they would not need to discuss laboratory errors and the risks of false negatives and positives. However, they should still be required to explain with whom the data might be shared, how it will be stored, and what data security and privacy measures will be taken to encrypt the data. Even where data can be uploaded anonymously with a pseudonym, users should be informed of the risks of re-identification by triangulating data from birth and death records and other accessible genetic databases.

Regardless of which mutations the consumers agree to have tested or shared, they should be given the DTC company's contact information (a phone number or email), which must be maintained so long as the company is marketing their services, where they can direct questions and be told how and with whom their information will be stored and shared in the future. The fact that U.S. law does not require any sort of informed consent for DTC genetic testing means that the quality of the consent processes vary considerably. Consumers are therefore only protected through consumer protection statutes, which are notoriously weak at preventing misrepresentation.[286]

While the specifics of what would be necessary for meaningful informed consent will need to be worked out in particular detail by others, we should at least agree that consumers need better information before they, perhaps naively, upload their genetic information online. We have mistakenly assumed that genetic information could be given directly to consumers, without the involvement of health care professionals. Unlike the measures

286. Samuel Issacharoff, *Group Litigation of Consumer Claims: Lessons from the U.S. Experience*, 34 TEX. INT'L L.J. 135, 140 (1999).

taken in Europe and elsewhere, we have also failed to require specific privacy and security protections for data shared online.

Millions of Americans have already submitted their SNP profiles to public sites like GEDMatch, exposing colossal amounts of personal data to strangers. The review of the DTC companies' consent processes reveals that many fall short of providing adequate information. That means that countless consumers are submitting their saliva or cheek cells, being tested, and then sharing their genetic information online, without appreciating the full risks of doing so. This is the true problem with FGG. The many privacy concerns advanced in opposition to FGG would largely subside if we made sure that consumers had meaningfully consented to the initial test, and that they had appreciated the volume of data contained in our genomes and how it was being shared. If consumers appreciated the privacy, security, and re-identification risks of genetic testing when they *first* submitted their saliva or blood sample, as well as when they then uploaded their data to a third-party site, we could feel more confident in law enforcement's use of this data in their investigation of crime. But our initial suspicions about the quality of the consumers' consent to DTC testing is spilling over into a misplaced concern about FGG. Coupled with our tendency to attribute intentionality to inanimate objects like DNA, to think that genetics plays a larger role in predicting our futures than the environment does, and to feel discomfort with not having control over who (or what) "speaks" for us, we have allowed far too much fear of genetic informants to take hold. Privacy advocates have misdiagnosed the problems with FGG and have thus proposed the wrong remedy—banning FGG. Rather than feeding into this unwarranted fear and banning the methodology, we must directly address the risks at their roots. We can do this by shoring up consent to DTC genetic testing and passing legislation aimed at prohibiting certain secondary uses of genetic data.

INSTRUCTIONS FOR USE:

1. Install the two included fonts on your system:
    a. Baskerville Italics.ttf
    b. Baskerville Normal.ttf
2. Open this template, then press Ctrl+S to save the new document before any material is added.
3. Update information on front page, including:
    a. Header (Remember, they are different on odd and even pages and both of them need it):
        i. Year
        ii. Volume
        iii. Short Article Title (all caps, but no brackets)

iv. Starting Page Number (Insert>Page Numbers>Format)
    1. The formatting on this has gotten weird in later versions of word. It's largely intuitive how to fix it, it's just incredibly important that it be fixed.
    2. Additionally, ensure that you appropriately end up on the odd/even header (odd has page number on right, even on left)

b. STLR Block
    i. Volume Number
    ii. Season and Year of Publication
c. Article Title
d. Author Name
e. Front Page Footnotes
    i. Author's information
    ii. Perma-link (URL where "article may be cited as")
        1. The perma-link has two variables, volume and article. The text that follows the = sign for each of those variable names is set as the variable. The & stops the interpreter and tells it another variable is coming. A perl script runs on the website that interprets those perma-links. BUT ONLY IF YOU SET THE VARIABLES RIGHT
            a. This perl script was in effect starting with Volume 16, prior volumes follow a different naming convention, and are dealt with in the script, accordingly.
        2. After "volume=" (with no spaces) type the Arabic numerals of the volume number this article is to be published in.
        3. After "article=" (with no spaces) type whatever name you gave to the pdf as it will be saved in filebase without the ".pdf" part (this should be the author's last name, but adjust if other articles in the current volume share that last name or if other necessities dictate)

4. Upload the article to the category for the current volume on filebase.
    a. So if Example.pdf in Volume 99, it would be saved in volumes/volume99 on file base
    b. Then it would have hyperlink http://www.stlr.org/cite.cgi?volume=99&article=example
    c. Institutional history should have a video that demonstrates how to do this, and how the perl script works.
    d. Make sure the splash page on the website reflects this URL.

4. Open the full "Styles" window by clicking on the drop-down arrow in the bottom right corner of the "Styles" box.
5. Paste abstract into template at the pre-specified location and set its style to Abstract.
6. Paste entire final version of the article (without markup & comments) into this template
7. Go through the entire text of the article (excluding footnotes) and apply the appropriate style to each portion:
    a. Heading 1 for high-level headings (I, II, III, etc.)
    b. Heading 2 for second-level headings (A, B, C, etc.)
    c. Heading 3 for third-level headings (1, 2, 3, etc.)
    d. Heading 4 for fourth-level headings (a, b, c, etc.)
    e. Heading 5 for fifth-level headings ((1), (2), (3), etc.)
    f. Body Text for all general text
    g. Block Quote for all block quotes
    h. Table Labels for all captions on tables and images
        i. Make sure any images are properly formatted, and centered.
    i. Hyperlinks for all URLs (make sure they are live, but that they look like plaintext)
8. Make sure headings renumber after each section (if they don't left click on the heading>Bullets and Numbering>Select Restart Numbering).
9. Make sure all footnote references use the footnote references style.
    a. Open the Advanced Find tool
    b. In the "Find what:" field type (without quotes): "^f"
    c. Select "main document" in the "Find In" dropdown menu
    d. Return to the main document, all the footnote numbers in the main document will be selected

    e. Click the "Footnote References" style
10. Make sure the footnotes are full justified (they should be if the Footnote Text style was properly applied, but I've been having trouble with that).
11. Go through footnotes to check for the following problems (and apply the solutions)
    a. URLs may cause the full justification to look awkward
        i. Press shift+enter between a / and a word in the URL (do not just press enter, that will break the link)
    b. The spaces between the § and the number in statute citations may cause the numbers and symbol to end up on different rows.
        i. Replace any spaces with a non-breaking space (press ctrl+space instead of just space)
12. Update the table of contents by right clicking on it and selecting "Update field," then "Update entire table." Only entries from Heading 1, 2, and 3 will be shown in the table of contents. Check them all for correct formatting, and use Shift+Enter to control the manner in which entries are split between lines. To add entries from subsequent headings, increasing the size of the table of contents substantially:
    a. Place the cursor at any point of the table of contents.
    b. Choose Insert>Index and Tables>Table of Contents>Change "show levels" to reflect the level of heading you want to include.
    c. Click OK when Word asks to replace the current table of contents
    d. NOTE: Bill changed the formatting of ToC headings so they should go to the next line a few spaces before hitting the page number. Double-Check that nonetheless.
13. Footnote numbers in the footnotes will, at this stage, show up as superscripts with no period or indentation. To format these correctly. I recommend saving a back-up copy of the document before this stage.:
    a. Press Ctrl+H and go to the "Find" tab
    b. In the "Find what:" field, type (without quotes): "^f"
    c. Click the "Find In" dropdown menu below and select "Footnotes"
    d. At this point, all footnote numbers in the footnotes themselves should be highlighted. BE VERY CAREFUL HERE, as changes may be difficult to undo. Click on the top of the main document

window, then press Ctrl+Space to strip the footnote numbers of their superscript formatting.

e. While all the footnote numbers (in the footnotes only) are still highlighted, go to the "Replace" tab in the "Find and Replace" window that should still be open and type the following string in the "Replace with:" field (without quotes): "^&.^t"
    i. "^&" signifies what was already selected
    ii. "." adds a period after that selection
    iii. "^t" adds a tab after the period
f. Click "Replace All" to set correct formatting.

14. Check for consistency throughout.
15. Delete these instructions and rejoice!