The Killer Inside Us: Law, Ethics, and the Forensic Use of Family Genetics

Joseph (Joe) Zabel*

A new era of criminal investigation has dawned in which decades-old cold cases are being solved through the forensic use of consumer genetic databases. Law enforcement increasingly harnesses the power of these databases to which individuals have uploaded their DNA in order to explore and understand their genealogy, health, and other highly personal attributes. By surreptitiously accessing these databases, law enforcement can track down criminal targets based on their family relation to any individuals populating the databases. While a growing number of cases have figured prominently in law enforcement's use of these databases—none has demonstrated the power and reach of these databases as much as the Golden State Killer case. As that case demonstrates, alongside this new genetic search capability, new legal and ethical concerns emerge. This article identifies, through the example of the Golden State Killer case, those concerns and proposes the kind of balancing test that a court encountering a legal challenge to the forensic use of direct-to-consumer databases should perform. This challenge has not yet been made, but when it is, the courts will have to balance the potent crime-solving benefits of genetic search technology against the privacy interests of the various affected individuals. In the process, this article also examines applicable legal doctrine from various cases in which courts have grappled with expansive and probing technologies and their threat to reasonable expectations of privacy. Central foci are the courts' mounting discomfort with the long-established third-party doctrine and, correspondingly, their

DOI: https://doi.org/10.15779/Z385D8NF71

* Joseph Zabel, Stanford Law School. I would like to thank the members of the Berkeley Journal of Criminal Law for their excellent suggestions and invaluable assistance. I would also like to extend my deep gratitude to Professor Robert Weisberg for his time and thoughtfulness, to my father, Richard Zabel for helping me throughout the development of this article, and to my friend, Emily Gruener for her insightful comments.

emerging embrace of the equilibrium-adjustment theory of Fourth Amendment jurisprudence pursuant to which courts redraw Fourth Amendment protections as technology becomes more invasive.

Introduction 48
The Science and Commerce of DNA Matching 50
The Third-Party Doctrine and DNA Matching 53
I. Mechanics of Commercial Genetic Database Searches 56
II. Statutory Framework 58
III. Harms Implicated by Forensic Genetic Searches 62
A. Databased Persons 62
B. Innocent Relatives Outside the Database 66
C. The Source/False Matches 70
D. Potential Harms of Genetic Searching 72
IV. Fourth Amendment Analysis 73
A. Searches of Databased Persons 74
1. Does the third-party doctrine obviate the government's need to obtain a warrant? 77
2. If the third-party doctrine does not obviate the government's need to obtain a warrant, is it still otherwise "reasonable" for the government to conduct the search without a warrant under the Riley balancing test? 86
B. Searches of Relatives of Databased Persons 89
V. Philosophical Considerations 92
Conclusion 97

INTRODUCTION

Joseph DeAngelo, a.k.a. the "Golden State Killer", was one of the most prolific and insidious serial killers in United States history. From 1974 to 1986, he traveled invisibly throughout California, hopping from city to city, known by different names in each—the "Visalia Ransacker," the "East Area Rapist," and the "Original Night Stalker."[1] Although his

[1] Avi Selk, *The Most Disturbing Parts of the 171-Page Warrant for the Golden State Killer Suspect*, WASH. POST (June 2, 2018, 1:55 PM), https://www.washingtonpost.com/news/post-nation/wp/2018/06/02/the-most-disturbing-parts-of-the-171-page-warrants-for-the-golden-state-killer-suspect/?noredirect=on&utm_term=.a55a6e915fa4 (describing in detail the nature and extent of the crimes committed).

alleged attacks became darker and more frequent as his criminal career progressed, law enforcement officers were still unable to identify him; he was deliberate, calculating, and careful not to leave a trace.[2] Frustrated by his ability to elude arrest, the FBI and local law enforcement agencies held a news conference on June 15, 2016 offering a $50,000 reward for DeAngelo's capture.[3] These efforts, even supplemented by law enforcement's searches of its own government genetic databases, were unsuccessful.[4]

While traditional investigative techniques could not catch up with the Golden State Killer (GSK), the steady advance of technology could. DeAngelo was finally caught—decades after his criminal career had ostensibly ended—through the use of a new investigative technique called forensic genetic genealogy.[5] In genetic genealogy, a user, normally looking to trace their lineage or connect with unknown family members, sends in a DNA sample (such as a saliva sample) to a direct-to-consumer (DTC) genetic database service like Ancestry.com or 23andMe.[6] These

---

[2] *Id.*

[3] *See* Press Release, FBI Sacramento, FBI Announces $50,000 Reward and National Campaign to Identify East Area Rapist/Golden State Killer (June 15, 2016), https://www.fbi.gov/contact-us/field-offices/sacramento/news/press-releases/fbi-announces-50-000-reward-and-national-campaign-to-identify-east-area-rapist-golden-state-killer ("[D]etectives . . . [can] quickly exclude innocent parties, and the public should not hesitate to provide information—even if it is the name or address of an individual who resided in the areas of the crimes—as many parties will be quickly excluded by a simple, non-invasive test.").

[4] Laura Miller, *How Did Police Find the Golden State Killer Suspect? Michelle McNamara's Researcher Has a Hunch.*, SLATE (Apr. 25, 2018, 10:03 PM), https://slate.com/news-and-politics/2018/04/paul-haynes-researcher-for-ill-be-gone-in-the-dark-on-how-police-found-the-golden-state-killer-suspect.html (noting that although "the crimes were committed before forensic science employed DNA analysis, investigators in the 2000s used [DNA analysis] to determine that the same man was responsible for both the East Area Rapist assaults and a series of home invasion rapes and murders in Southern California").

[5] Chris Phillips, *The Golden State Killer Investigation and the Nascent Field of Forensic Genealogy*, 36 FORENSIC SCI. INT'L.: GENETICS 186, 186-88 (2018) (commenting on the potential of this field and its likely expansion in service of law enforcement); Paige St. John, *Death Penalty Sought for Golden State Killer Suspect*, L.A. TIMES (Apr. 10, 2019, 3:31 PM), https://www.latimes.com/local/lanow/la-me-golden-state-killer-death-penalty-20190410-story.html (observing that prosecutors are now seeking the death penalty for GSK despite California's moratorium preventing executions from being carried out in the state).

[6] Sarah Zhang, *How a Tiny Website Became the Police's Go-To Genealogy Database*, The ATLANTIC (June 1, 2018), https://www.theatlantic.com/science/archive/2018/06/gedmatch-police-genealogy-

services provide the user with a genetic profile.[7] The user will then upload the profile obtained from their chosen service to GEDmatch, a free open-source public aggregator that allows the user to match with people on many different sites—not only the particular service they initially chose.[8] GEDmatch searches for sections of the user's chromosomes that match other users in the database and provides usernames and contact information for any genetic matches it finds, along with an estimation of how closely related the matches are.[9]

The Science and Commerce of DNA Matching

Law enforcement officers follow the same procedure in uploading DNA to GEDmatch as do regular users, but instead of submitting their own genetic profiles to GEDmatch, officers submit DNA recovered from an unidentified crime suspect or victim, often left at a crime scene. GEDmatch then "reports back a list of 'hits'—users who share DNA with the unidentified target."[10] Investigators examine those hits to try to ascertain the identity of the perpetrator of the crime. They work from the list of hits, running information through public record databases to grow family trees based on the original hits in an attempt to find leads which ultimately yield their target's identity.[11] Investigators must then use other means to confirm that the DNA from the discovered target matches DNA found at the scene of the crime.[12] If completed correctly, a match may very well mean "case closed" as a matter of scientific certainty.

This method cracked the Golden State Killer case. Through familial searching on GEDmatch, investigators identified distant relatives of DeAngelo—including family members directly related to his great-

database/561695.

[7] *Id.*

[8] *Id.* (noting that GEDmatch will have profiles from individuals who used sites such as 23andMe and Ancestry).

[9] Family History Fanatics, *Getting Started with GEDmatch – A Segment of DNA*, YOUTUBE (Sept. 3, 2019), https://www.youtube.com/watch?v=id7JJ1NoTNk&feature=youtu.be (explaining the process of uploading raw data to GEDmatch).

[10] Ericka Check Hayden, *Genetics Extends the Long Arm of the Law*, KNOWABLE MAG. (Jan. 18, 2019), https://www.knowablemagazine.org/article/technology/2019/genetics-extends-long-arm-law (showing that at this point, law enforcement knows that the hits themselves are not the perpetrators because the test shows that these individuals share enough DNA with the source of the DNA to be related to the source, but not enough to be the source themselves).

[11] *Id.*

[12] *Id.*

great-great-great grandfather dating back to the 1800s.[13] Based on this information, investigators built about 25 different family trees.[14] The tree that eventually linked to the Golden State Killer alone contained approximately 1,000 people.[15] Over the course of a few months, investigators used other clues like age, sex and place of residence to rule out suspects populating these trees, eliminating suspects one by one until only DeAngelo remained.[16]

Law enforcement's access to direct-to-consumer databases raises unique ethics concerns. As of April 2019, GEDmatch has made 1.2 million genetic profiles available to law enforcement.[17] Other DNA-testing companies, such as FamilyTree DNA, share their consumer data on nearly 2 million genetic profiles with federal law enforcement.[18] The genetic information contained in these databases provides investigators with links to hundreds of millions of people who are related to the individuals who created the genetic profiles and potentially even more as the technology advances.[19] Law enforcement may search a DTC database to obtain a familial match without a warrant or any judicial or regulatory oversight and officers may identify and potentially track even distant relatives of individuals who decided to use commercial databases.[20] This

---

[13] Justin Jouvenal, *To Find Alleged Golden State Killer, Investigators First Found His Great-Great-Great-Grandparents*, WASH. POST (Apr. 30, 2018, 3:22 PM), https://www.washingtonpost.com/local/public-safety/to-find-alleged-golden-state-killer-investigators-first-found-his-great-great-great-grandparents/2018/04/30/3c865fe7-dfcc-4a0e-b6b2-0bec548d501f_story.html?utmterm=.6c802477b539.

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] Peter Aldhous, *We Tried To Find 10 BuzzFeed Employees Just Like Cops Did For The Golden State Killer*, BUZZFEED NEWS (Apr. 9, 2019, 9:16 AM), https://www.buzzfeednews.com/article/peteraldhous/golden-state-killer-dna-experiment-genetic-genealogy (identifying six of ten BuzzFeed employees through GEDmatch).

[18] Kristen V. Brown, *A Major DNA-Testing Company Is Sharing Some of Its Data With the FBI. Here's Where It Draws the Line*, FORTUNE (Feb. 1, 2019), http://fortune.com/2019/02/01/genetic-testing-consumer-dna-familytreedna-fbi/.

[19] *Id.*

[20] *GEDmatch.com Terms of Service and Privacy Policy*, GEDMATCH.COM, https://www.gedmatch.com/tos.htm (last updated May 18, 2019) ("There are 4 classes of DNA data on this Site: 'Private', 'Research', 'Public + opt-in' and 'Public + opt-out' . . . . 'Private' DNA data is not available for comparisons with other people. It may be usable in some utilities that do not depend on comparisons with other DNA. 'Public + opt-in' DNA data is available for comparison to any Raw Data in the GEDmatch database using the various tools provided for that purpose. 'Public + opt-out' DNA data is available for

is true despite the fact that these distant relatives never consented to the upload of their genetic information and may explicitly wish to be left alone from the world of databases and digital identity. For them, there is no opt out.

Up until May 2019, law enforcement could search GEDmatch to obtain a familial match as long as the suspect whose DNA they uploaded was suspected of either murder or sexual assault.[21] Individuals, by default, made their profiles available to law enforcement upon upload.[22] Then, in May 2019, GEDmatch changed its terms of service in two meaningful ways. GEDmatch permitted law enforcement to use its services to find and apprehend a 17-year-old high-school student who assaulted a 71-year-old woman inside a Mormon church, a crime that did not involve sexual assault or murder, but was one for which GEDmatch bent its own rules and allowed police access to its database because the elderly woman was reportedly afraid the assailant would eventually kill her.[23] Following that and the public outcry engendered by GEDmatch's decision to violate its own terms of service, GEDmatch updated its terms of service such that users now have to affirmatively opt in if they want to allow law-enforcement officials to have access to their data. However, importantly, relatives of those users still have no say in the matter at all.[24] GEDmatch

comparison to any Raw Data in the GEDmatch database, except DNA kits identified as being uploaded for Law Enforcement purposes. Comparison results, including your kit number, name (or alias), and email will be displayed for 'Public' kits that share DNA with the kit being used to make the comparison, except that kits identified as being uploaded for Law Enforcement purposes will only be matched with kits that have 'opted-in'. 'Research' DNA data is available for one-to-one comparison to other Public or Research DNA. It is not shown in other people's 'one-to-many' results lists. The Raw Data that you uploaded is not made available. By default, your Raw Data is not available to any user of the Site - not even you. However, you understand that anyone with the kit number for Raw Data can perform many or all of the same GEDmatch functions with that Raw Data that the provider of that Raw Data can perform.").

[21] *See* Dick Eastman, *The Reasons Why GEDmatch Recently Changed Its Terms of Service*, EASTMAN'S ONLINE GENEALOGY NEWSLETTER (May 27, 2019), https://blog.eogn.com/2019/05/27/the-reasons-why-gedmatch-recently-changed-its-terms-of-service/.

[22] *Id.*

[23] Barbie Latza Nadeau, *Did GEDmatch's New DNA Rules Just Freeze Out Cold-Case Murder Investigators?*, DAILY BEAST (May 20, 2019, 8:51 AM), https://www.thedailybeast.com/gedmatch-genealogy-databases-new-terms-will-make-it-harder-for-cops-to-close-cold-cases.

[24] *See GEDmatch.com Terms of Service and Privacy Policy*, *supra* note 20. It is unclear whether and the extent to which law enforcement would have to abide by a user's decision not to opt in. Moreover, there is a growing movement led by some genealogists to

also changed its terms of service to more liberally permit law enforcement access to GEDmatch for a significantly greater range of crimes, including non-negligent manslaughter, robbery, and aggravated assault.[25] Such a change may well portend the expansion of forensic genetic searching to crimes of lesser and lesser severity.

Despite these changes, use of genetic databases is still increasing. GEDmatch has become immensely popular, with well over a million users as of November 2018—a number which is still increasing rapidly.[26] Meanwhile, more than 15 million people have submitted their DNA to other online genealogy services in recent years.[27] In less than three years, geneticists predict that the DNA of 90 percent of Americans of European descent will be identifiable through relatives on GEDmatch's database even if they have not submitted their own DNA.[28] Eventually every American will be genetically identifiable.[29]

The Third-Party Doctrine and DNA Matching

DNA matching technology, while inarguably useful for investigators, is generally unrestrained by judicial oversight and destined to face a legal challenge soon. This is especially true given that, in recent years, the United States Supreme Court has demonstrated discomfort with the pressure that emerging technology, when in the service of law

convince users of GEDmatch to opt in. *See* Jon Schuppe, *Police Were Cracking Cold Cases with a DNA Website. Then the Fine Print Changed*, NBC NEWS (Oct. 23, 2019, 4:19 PM), https://www.nbcnews.com/news/us-news/police-were-cracking-cold-cases-dna-website-then-fine-print-n1070901 ("Th[e] sharp drop in the usefulness of a promising technology has sparked an effort by law enforcement authorities and researchers . . . to convince the public to take action. These groups hope to persuade more Americans to obtain their DNA profiles from direct-to-consumer genetic testing companies ─ most of which have large databases but don't allow law enforcement searches ─ and share them publicly, including with law enforcement, on databases like GEDmatch.").

[25] *See* Nadeau, *supra* note 23.

[26] Jorge Milian, *Cold-Case Murders, Rapes Cracked by Lake Worth Genealogy Website*, PALM BEACH POST (Nov. 29, 2018, 10:32 AM), https://www.palmbeachpost.com/news/20181129/cold-case-murders-rapes-cracked-by-lake-worth-genealogy-website.

[27] 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.

[28] *Id.*

[29] *Id.* (noting that Americans of Northern European descent are most identifiable because they are the primary users of commercial genetic databases at this time).

enforcement, has put on traditional notions of privacy.[30] For decades, without having to satisfy Fourth Amendment requirements, law enforcement has freely had access to individuals' unique personal information so long as that information was willingly turned over to a third party.[31] Recently, however, because certain technologies now enable nearly constant surveillance of individuals' actions based on information those individuals surrender to third parties, the Supreme Court has begun to retreat from its traditional orthodoxy that there is no reasonable expectation of privacy in information willingly given to a third party.[32]

The erosion of the third-party doctrine began in 2012 in *United States v. Jones* where, even though the Court based its ruling on a government trespass through the installation of a GPS device, certain Justices were clearly troubled by the constancy of surveillance enabled by the device.[33] The Court's concern that mechanical adherence to the third-party doctrine could lead to a creeping surveillance state deepened in 2018 in *Carpenter v. United States*.[34] In *Carpenter*, the Court held that the government violated the Fourth Amendment by accessing cellphone records in the possession of third-party cellphone providers without a search warrant because such records revealed the continuing physical locations of an individual's cellphone.[35] In so holding, the Court began to redraw old concepts of privacy by establishing new protections against the warrantless disclosure of certain publicly cognizable information.

The Court's concern over law enforcement's previously unbridled access to cellphone and GPS data raises questions about law enforcement's currently unfettered access to direct-to-consumer genetic databases. Law enforcement has used DNA information—obtained without a warrant—to track down criminal suspects by matching the

---

[30] *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206 (2018); Riley v. California, 573 U.S. 373 (2014); United States v. Jones, 565 U.S. 400 (2012) (all challenging the government's use of probing technologies that implicate privacy concerns).

[31] *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743-44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

[32] *See, e.g.*, Carpenter, 138 S. Ct. at 2206 (holding that in order to access certain cell phone data reposed to a third party, a showing should be required).

[33] 565 U.S. at 404 (holding "that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search'").

[34] *See* 138 S. Ct. at 2206.

[35] *Id.* at 2220 (noting that the Court does not hold on whether fewer days of cell site location information could be accessed by law enforcement without a warrant).

suspect's genetic information or the genetic information of a suspect's family members on the database with DNA evidence found at the scene of a crime. Meanwhile, companies such as Parabon Nanolabs have offered their affirmative assistance to law enforcement in conducting tests on DTC databases, claiming that they can identify criminal suspects as distant as ninth-degree relatives. Law enforcement has taken full advantage of these services.[36] In 2018 alone, law enforcement used GEDmatch (in many cases with assistance from Parabon Nanolabs) to find suspects in a total of 28 cold murder and rape cases.[37]

While individuals who upload information to a searchable public database have in many ways waived their rights to such privacy, this was also the case with respect to cell phone records before *Carpenter*.[38] Nevertheless, the Court pared back the third-party doctrine with regard to cell phones and held that the records of those phones, previously obtainable without a warrant, required a warrant under circumstances where the search is highly intrusive in terms of its magnitude.[39] The issue of the contours of the third-party doctrine in the face of new technology, and particularly genetic testing, is not settled and in fact may just be developing. Indeed, the increasing public scrutiny that consumer genetics has faced as an industry may accelerate forthcoming legal challenges.

This article examines the legal and ethical implications of forensic DTC genetic database searches, discussing the state of the law as well as privacy and other moral concerns evoked by this new technology. As a preliminary matter, it provides a technical background on how DTC databases work. This article describes the legal landscape as applied to this technology at both the federal and state level. It then identifies and examines the harms incurred by individuals during various stages of a genetic database investigation. It explores whether a person's genetic information is sufficiently private to justify a reasonable expectation of privacy under the Fourth Amendment. It discusses how a person's use of a genetic database may or may not fit within the third-party doctrine as it

---

[36] 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.

[37] Robert Gearty, *DNA, Genetic Genealogy Made 2018 the Year of the Cold Case: 'Biggest Crime-Fighting Breakthrough in Decades'*, FOX NEWS (Dec. 19, 2018), https://www.foxnews.com/us/dna-genetic-genealogy-made-2018-the-year-old-the-cold-case-biggest-crime-fighting-breakthrough-in-decades.

[38] 138 S. Ct. at 2213.

[39] *Id.* at 2221.

stands after *Carpenter*, and how the third-party doctrine and reasonable expectations of privacy co-exist. After that, this article navigates the philosophical considerations surrounding the forensic exploitation of these databases, applying normative principles outside of Supreme Court doctrine. Finally, this article concludes with an examination of possible avenues to mitigate the privacy harms potentially inflicted by this technology and an overview of the ethical and legal balancing necessary on this issue. Such a balancing weighs the crime-solving benefits of the technology against the various harms the technology imposes on different actors throughout the investigative process. Ultimately, if the degree to which DTC databases intrude on privacy is greater than the degree to which law enforcement needs to use these databases to solve crimes, law enforcement should not be allowed to use the technology to solve crimes.

I. MECHANICS OF COMMERCIAL GENETIC DATABASE SEARCHES

There are two types of genetic databases in the United States: government and commercial. The government uses its databases to retain biological information collected from persons convicted of and arrested for crimes at the local, state, and federal level.[40] CODIS, an acronym for the Combined DNA index system, is the national database maintained by the FBI.[41] The FBI is authorized to upload DNA from those convicted of a crime, charged in an indictment and "other persons whose DNA samples are collected under applicable legal authorities."[42] "CODIS also maintains a database of more than half a million *unidentified* DNA samples from crime scenes," to which investigators turn if they do not find a match in the named samples.[43]

Government databases use "short tandem repeats" (STR) analysis to test DNA samples.[44] When using a genetic database, investigators first determine a suspect's STR profile from, for example, blood, semen or

[40] JULIE E. SAMUELS ET AL., URBAN INST., COLLECTING DNA FROM JUVENILES 1-2 (2011) (noting that some local databases collect DNA samples of arrestees who have not been convicted).

[41] *Id.* at 2.

[42] 34 U.S.C. § 12592(a)(1) (2017).

[43] Ricki Lewis, *Genetic Privacy and the Case of the Golden State Killer—Diving into the Science*, GENETIC LITERACY PROJECT (May 1, 2018), https://geneticliteracyproject.org/2018/05/01/genetic-privacy-and-the-case-of-the-golden-state-killer-diving-into-the-science/.

[44] Karen Norgaard, *Forensics*, *DNA Fingerprinting, and CODIS*, 1 NATURE EDUCATION 35 (2008).

tissue from a crime scene, then compare it to database records.[45] STR analysis compares specific locations on DNA from two or more samples and notes variations in the number of repetitions of nucleotides (components that make up DNA).[46] The analysis is purportedly intentionally limited; it can be used to identify individuals or close relatives of an individual, such as a suspect's parent, child, or sibling, but not much else about those individuals or their more distant relatives.[47]

Privately-owned databases (DTC databases), on the other hand, employ a newer type of analysis called single-nucleotide polymorphisms (SNP) analysis.[48] In the case of DTC databases, individuals voluntarily provide DNA samples used for the SNP analysis in order to receive information about their genealogy. SNP analysis reveals not only how related one individual is to another but also insights into that individual's ancestry, eye color, medical history and propensity to develop genetic diseases.[49] Therefore, if investigators are unable to find an exact match or any close relatives of their target in CODIS, DTC databases provide a far more powerful tool for analytical purposes. GEDmatch for instance, contains information for individuals on "100,000 to 600,000 genetic markers," a degree of numerosity and precision that CODIS lacks.[50] This numerosity reveals far more attenuated genetic relatives than the STR analysis employed in the CODIS database does.[51]

The government uses STR analysis, as opposed to SNP analysis, ostensibly because it is not supposed to reveal much biological information.[52] In CODIS, the uploaded profiles "consist solely of the

---

[45] *Id.*

[46] *Id.*

[47] Erin Murphy, *Law and Policy Oversight of Familial Searches in Recreational Genealogy Databases*, 292 FORENSIC SCI. INT'L e5, e6 (Aug. 31, 2018) [hereinafter Murphy, *Law and Policy*]. As it turns out, this is not an accurate description of the limits of STR because scientists are now able to essentially convert an STR profile into a more robust one that shows much more about an individual. *See, e.g.*, Michael Edge et al., *Linkage Disequilibrium Matches Forensic Genetic Records to Disjoint Genomic Marker Sets*, 114 PROC. NAT'L ACAD. SCI. 5671, 5675 (2017).

[48] Murphy, *Law and Policy*, *supra* note 47, at e5.

[49] *See* Zhang, *supra* note 6; *see also* Robert Wyttenbach, *Relatedness*, CORNELL HOLY LAB (2012) (shared DNA is proportional to the degree of relatedness between two individuals, so it serves as an accurate proxy for determining biological relationships).

[50] *See* Hayden, *supra* note 10.

[51] *See* Murphy, *Law and Policy*, *supra* note 42 at e5.

[52] *See, e.g.*, Maryland v. King, 569 U.S. 435, 463 (2013) ("[T]he CODIS loci come from noncoding parts of the DNA that do not reveal the genetic traits of the arrestee. While science can always progress further, and those progressions may have Fourth Amendment

numbers describing the alleles, as well as identifying information that allows the record to be traced back to the uploading entity."[53] Law enforcement may only collect and analyze the non-coding portions of the genome.[54] The DNA evidence collected by the government is, in essence, "a string of numbers—[that] doesn't reveal anything personally identifiable on its own."[55] The lack of highly intrusive personally identifiable information available to the government from a DNA swab is critical to the constitutionality of the search. This lack of information is the basis on which the Supreme Court has allowed police officers to take DNA from mere arrestees without violating the Fourth Amendment.[56] However, a new study demonstrates that STR data (for instance from CODIS) can actually reveal genetic traits when matched up with an ancestry archive like GEDmatch.[57] These databases can be cross-referenced and an STR profile can be effectively converted into an SNP profile.[58] This means that the half a million unidentified individuals in CODIS could potentially be identified in a commercial genetic database. Thus, the "practical firewall" between offender databases such as CODIS and commercial genetic databases is coming down.[59]

II. STATUTORY FRAMEWORK

There is little legal process and no real boundaries around the forensic exploitation of consumer genetics by law enforcement in DTC databases. In fact, as a *Los Angeles Times* investigation recently uncovered: "there is actually no uniform approach for when detectives turn to genealogical databases to solve cases."[60] The investigation found

consequences, alleles at the CODIS loci 'are not at present revealing information beyond identification.' The argument that the testing at issue in this case reveals any private medical information at all is open to dispute.").

53 Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291, 296 (2010) [hereinafter Murphy, *Relative Doubt*].

54 Megan Molteni, *Genome Hackers Show No One's DNA Is Anonymous Anymore*, WIRED (Oct. 11, 2018, 2:04 PM), https://www.wired.com/story/genome-hackers-show-no-ones-dna-is-anonymous-anymore/ [hereinafter Molteni, *Genome Hackers*].

55 *Id.*

56 *See King*, 569 U.S. at 465.

57 *See* Edge, *supra* note 47, at 5672.

58 *Id.*

59 Molteni, *Genome Hackers*, *supra* note 54.

60 Paige St. John, *DNA genealogical databases are a gold mine for police, but with few rules and little transparency*, L.A. TIMES (Nov. 24, 2019, 5:00 AM), https://www.latimes.com/california/story/2019-11-24/law-enforcement-dna-crime-cases-privacy?utm_source=The+Appeal&utm_campaign=6227545180-

that while "in some departments, [searches of DTC databases] are to be used only as a last resort . . . [o]thers are putting them at the center of their investigative process . . . [while] some like Orlando, have no policies at all."[61] Moreover, even when law enforcement has used DTC databases, they have shrouded their use in secrecy, declining to "provide details to the public, including which companies detectives got the match from."[62] Because of this secrecy, it has become "difficult to understand the extent to which privacy was invaded, how many people came under investigation, and what false leads were generated."[63]

In contrast, CODIS searches and other government databases are regulated to a much greater extent by federal and state laws. Federal law enforcement agencies are generally prohibited from performing familial DNA searching.[64] States and localities vary much more.[65] In California, for instance, investigators must get approval from "a state Department of Justice committee to run a familial DNA search through a criminal [government] database, which limits use of the technique to particularly heinous crimes."[66] A similar search on a private site like GEDmatch

EMAIL_CAMPAIGN_2018_08_09_04_14_COPY_01&utm_medium=email&utm_term=0_72df992d84-6227545180-58431075.

[61] *Id.*

[62] *Id.*

[63] *Id.*

[64] Susan Scutti, *You Might Not be Anonymous, Thanks to Genealogy Databases*, CNN (Oct. 11, 2018, 3:47 PM), https://www.cnn.com/2018/10/11/health/genetic-privacy-study/index.html. An exception can be made when law enforcement conducts a "moderate stringency search." *Frequently Asked Questions on CODIS and NDIS*, FED. BUREAU INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet (last visited Jan. 8, 2019) (defining a moderate stringency search as a "means of searching forensic profiles from crime scene evidence that contains DNA from more than one individual" which can yield biological relatives).

[65] Local law enforcement may operate their own DNA databases with much less regulatory oversight. *See, e.g.*, Jan Ransom & Ashley Southall, *N.Y.P.D. Detectives Gave a Boy, 12, a Soda. He Landed in a DNA Database*, N.Y. TIMES (Aug. 15, 2019), https://www.nytimes.com/2019/08/15/nyregion/nypd-dna-database.html ("A growing number of law enforcement agencies throughout the country — including police departments in Connecticut, California and Maryland — have amassed genetic databases that operate by their own rules, outside of state and federal guidelines, which tend to be far more strict.").

[66] Megan Molteni, *The Creepy Genetics behind the Golden State Killer Case*, WIRED, (Apr. 27, 2018, 4:00 PM), https://www.wired.com/story/detectives-cracked-the-golden-state-killer-case-using-genetics/ [hereinafter Molteni, *Creepy Genetics*]; *see also* Madison Pauly, *Police Are Increasingly Taking Advantage of Home DNA Tests. There Aren't Any Regulations to Stop It*, MOTHERJONES (Mar. 12, 2019),

requires no such oversight.[67] This may be due to the accepted wisdom that the third-party doctrine, which holds that data voluntarily conveyed to a third party (as is the case when one uses GEDmatch), applies wholesale to the police use of genetic databases. Therefore, under this reasoning, law enforcement's genetic searching is not subject to Fourth Amendment protection.

As of the writing of this article, there has been one trial and subsequent conviction in a cold case in which the defendant was found with the assistance of DTC database searching. This was the case against William Talbott II, who was convicted for the 1987 murder of a young Canadian couple who disappeared during an overnight trip to Seattle. The couple's bodies were discovered in a rural part of western Washington after their disappearance. In order to find the killer, "investigators . . . trace[d] semen left at one of the crime scenes to Talbott through two cousins who had uploaded their own genetic information to a public database called GEDMatch."[68] This case represents "the first 12-person vote of confidence in genetic genealogy's ability to not just put a name to a drop of blood or skin cells lifted from a fingerprint or a semen-soaked swab, but to help prosecutors prove that the person behind that name also committed the crime" of which they have been accused.[69] Nevertheless, there has not yet been a Fourth Amendment challenge to law enforcement's use of DTC platforms.[70] Indeed, the defense in the Talbott case could "have challenged the use of genetic genealogy on privacy grounds, or as a violation of people's right to control their personal data . . . [but] [i]nstead, [the] defense lawyers did not pose a single question about the technique."[71] Following the conviction, genealogist

https://www.motherjones.com/crime-justice/2019/03/genetic-genealogy-law-enforcement-golden-state-killer-cece-moore/?fbclid=IwAR3lOZl6fAtkNdgYE5umtSgxz1qbbaS5_aOU9j7eGJHv68UY_JOX2MRw6EM (noting that in 2019, a bill was proposed in Maryland to prohibit law enforcement from using its databases for crime solving, but the bill did not pass).

67 Molteni, *Creepy Genetics*, *supra* note 66.

68 Megan Molteni, *Man Found Guilty in a Murder Mystery Cracked By Cousins' DNA*, WIRED (June 29, 2019, 3:05 PM), https://www.wired.com/story/man-found-guilty-in-a-murder-mystery-cracked-by-cousins-dna/.

69 *Id.*

70 TCR Staff, '*No Stopping Genetic Genealogy' After First Conviction*, THE CRIME REPORT (July 1, 2019), https://thecrimereport.org/2019/07/01/genet-genealogy-leads-to-first-conviction/; *see also* St. John, *supra* note 60 ("[T]he defense lawyer there agreed not to challenge the GEDmatch work that led police to her client.").

71 Heather Murphy, *Genealogy Sites Have Helped Identify Suspects. Now They've Helped Convict One.*, N.Y. TIMES (Jul. 1, 2019),

CeCe Moore said: "There is no stopping genetic genealogy now . . . I think it will become a regular, accepted part of law enforcement investigations."[72]

Additionally, there have been two subsequent developments in Florida and California, respectively, which have weakened the protections instituted by GEDmatch and potentially those of other DTC databases as well. In October 2019, following GEDmatch's policy changes, a Florida detective made public what had previously been only private. He had obtained a search warrant a few months earlier to search the full GEDmatch database (including individuals who had not opted in to allow law enforcement to view their data).[73] The court-approved warrant is essentially without limitation, and thus represents a potentially major privacy intrusion, the precise kind that privacy advocates have long lamented.[74] In fact, "DNA policy experts said the development was likely to encourage other agencies to request similar search warrants from 23andMe, which has 10 million users, and Ancestry.com, which has 15 million."[75] Previously, law enforcement had been hesitant to try to obtain court orders to penetrate DTC databases because "if users get spooked and abandon the sites, they will become much less useful to investigators."[76] The warrant, while now publicly available, has only been made public subject to numerous redactions—including the probable cause section— which, as discussed later in this article, would normally be difficult to satisfy.[77]

Despite the public announcement of the successful warrant in Florida, elsewhere law enforcement has been trying to circumvent privacy protections in DTC databases more surreptitiously. In California, for example, prosecutors persuaded a judge to treat genetic matches obtained from DTC databases as "confidential informants."[78] This treatment

https://www.nytimes.com/2019/07/01/us/dna-genetic-genealogy-trial.html.

[72] *Id.*

[73] Kashmir Hill & Erin Murphy, *Your DNA Profile is Private? A Florida Judge Just Said Otherwise*, N.Y TIMES (Nov. 5, 2019), https://www.nytimes.com/2019/11/05/business/dna-database-search-warrant.html.

[74] St. John, *supra* note 60.

[75] Hill & Murphy, *supra* note 73.

[76] *Id.*

[77] Orlando Police Department Search Warrant in the Circuit Court for the Ninth Judicial District in and for Orange County, Florida, https://www.documentcloud.org/documents/6547788-Orlando-PD-Search-Warrant-for-GEDMatch.html.

[78] St. John, *supra* note 60; People v. Waller, No. 18FE018342, Order Granting

enables law enforcement to essentially "seal searches so consumers are not scared away from adding their own DNA to the forensic stockpile."[79] Moreover, as reported by the *Los Angeles Times*, "genealogy searches remain sealed elsewhere in California, Texas and Florida."[80]

III. HARMS IMPLICATED BY FORENSIC GENETIC SEARCHES

DTC database searches of commercial genetic databases pose harms to three separate but related categories of persons: (1) the databased persons, also called the "pivots," "leads," or the "genetic informants" whose partial match with evidence taken from a crime scene leads police to investigate other members of their family, (2) perhaps most significantly, those other members of the family whom the police find, investigate, and from whom they may obtain DNA samples, and, (3) the source(s) of genetic information left at the crime scene themselves.

A. Databased Persons

The first harm is inflicted on persons who have uploaded their genetic information to a database such as GEDmatch. The vast majority of these people have not committed the subject offense or even any offense at all.[81] However, a significant number of people are likely related to individuals who *have* committed serious crimes. This becomes truer and truer as genetic matches are made between relatives further and further apart as a matter of simple probability.[82] One individual, who completed the test herself with 23andMe, matched with 1,388 genetic relatives on the company's database. Her closest relatives on the site were third cousins, whereas her weakest matches were far more distant cousins.[83]

Databased persons may then be implicated in a criminal

Discovery Motion to Protect Official Information Pursuant to Evidence Code §1040 (2019).

[79] *Id.*

[80] *Id.* ("California prosecutors have also begun collaborating with a Texas genealogy company at the outset of what became a $2-million campaign to spotlight the heinous crimes they can solve with consumer DNA. Their goal is to encourage more people to make their DNA available to police matching.").

[81] *See, e.g.*, FED. BUREAU INVESTIGATION, U.S. DEP'T OF JUSTICE, UNIFORM CRIME REPORT: CRIME IN THE UNITED STATES 2013 (Fall 2014) (finding that in 2013, there occurred only 4.5 murders per 100,000 people in the United States).

[82] *See* Ram, *supra* note 36 (describing how distant relatives can be identified).

[83] Abigail Hoglund-Shen, *Direct-to-Consumer Genetic Testing, Gamete Donation, and the Law*, 55 FAM. COURT. REV. 472, 474 (2017).

investigation through one of these relatives. If some piece of genetic information is uploaded to GEDmatch, it will likely match with at least a few profiles.[84] If, as were the circumstances surrounding the Golden State Killer, the investigators' case has gone cold, any databased individual who is matched becomes an invaluable source of information, because one of their relatives is now known to be the perpetrator.[85] As a result, uploaders are subjected to police scrutiny based solely on the misdeeds of a relative.

The first harm resulting from such scrutiny is harm by association. When a relative is matched to a perpetrator's DNA, inevitably the relative is now associated to some degree with the offender.[86] Depending on how public the case is and how protective of the information investigators are, this association could become known. If the association is made public, the harms are obvious—no one wants to be affiliated with a serious criminal, even less so when that association is based on blood. If the association remains under wraps, then the harm of public embarrassment is less severe, but harm still exists for the associated individual if contacted by the police.

The association may also dredge up things about the family of databased persons that they did not want to know, such as their relationship to a criminal, that their parents are not their biological parents, or that they were conceived through an adulterous or incestuous relationship; these are just a few examples of the many painful circumstances that can emerge from genetic investigation. Further, they may be approached and sought as a witness by law enforcement, which may cause law enforcement to investigate their background and private life with an eye towards whether they might be a possible co-conspirator or accessory to the crime. Perhaps investigators will try to find them in CODIS imposing on them the additional harm and scrutiny by association and the reemergence of their past criminal behavior. All of this activity

---

[84] Yaniv Erlich et al., *Identify Inference of Genomic Data Using Long-Range Familial Searches*, 362 SCI. MAG. 690 (2018) (estimating that 60% of Americans of Northern European descent can be identified through familial DNA searching).

[85] Gina Kolata & Heather Murphy, *The Golden State Killer is Tracked Through a Thicket of DNA, and Experts Shudder*, N.Y. TIMES (Apr. 27, 2018), https://www.nytimes.com/2018/04/27/health/dna-privacy-golden-state-killer-genealogy.html.

[86] *See*, *e.g.*, Jennifer Bucholtz, *Identifying the Golden State Killer*, IN PUBLIC SAFETY (May 31, 2018), https://inpublicsafety.com/2018/05/identifying-golden-state-killer-investigator-details-role-ancestry-site/ (reporting the mistaken attribution of an Oregon man who shared relatives with the GSK).

has the potential to stigmatize them at a minimum merely because they submitted personal information for a highly personal and limited purpose.

The second harm incurred by the *databased* person is the cost imposed by being a part of an investigation. When someone is implicated in an investigation, they may be approached by law enforcement, often for assistance with the investigation. Police may try to find them in CODIS, which imposes the additional harm of the reemergence of their past criminal behavior. If they are searched in CODIS or other law enforcement databases and found to have a legal vulnerability such as a probation violation, an immigration issue or some unpaid fine, law enforcement may exploit that to gain cooperation against their relative.[87] This creates pressure, risk, and legal expense for them, all because of a private genetic search. Of course, they would not have to agree to assist, but law enforcement could then move to prosecute the individual more harshly than they might have otherwise, ultimately dangling benefits to relieve the pressure they created.[88] And even without legal vulnerability, law enforcement could subpoena the individual later on if it would be helpful in the investigation, at which point they would be required to assist whether they wanted to or not.[89] Lastly, they may be put in legal peril not only because of the crime being investigated, but simply because of unrelated legal vulnerabilities in their own life which are now exposed.

Finally, there is the harm imposed upon the dignity of a databased person when law enforcement conduct an unauthorized search of their private information. The individual's private information may have been provided for a very limited and private purpose, but is being accessed for other purposes without really any showing being made at all connecting the individual to a past or ongoing crime. Genetic information is often considered deeply personal and private by people, not only because it can identify a person, but also because "[i]t is fundamental and basic to our make-up."[90] People may feel harmed knowing that law enforcement officers are viewing their genetic profiles, even if law enforcement does nothing further with their profile. This is reminiscent of victims of burglaries who say that the greatest harm they felt was that a stranger was in their private domain regardless of whether any property was taken. The

---

[87] *See* U.S. DEP'T OF JUSTICE, U.S. ATTORNEYS' MANUAL § 9-27.600 (2018) (describing prosecutors' options when a witness refuses to cooperate).

[88] *Id.*

[89] *Id.*

[90] Sonia M. Suter, *Disentangling Privacy from Property: Toward a Deeper Understanding of Genetic Privacy*, 72 GEO. WASH. L. REV. 737, 773-74 (2004).

fact that the government has free license to look at one's genetic information might be a similar harm to one's dignity.

These harms may sound abstract, but they were substantial enough for the Supreme Court in *Carpenter* to proscribe law enforcement's access to historical cell-site location information. The decision in *Carpenter* ascribes a unique privacy and dignitary right to a cell phone because a cell phone is almost a "feature of human anatomy."[91] The Court analogizes the cell phone to a body part because it is with us at all times, and it contains an immense amount of private information including one's location that, if exposed, would provide "an intimate window into a person's life" and be a direct affront to our dignity.[92] Similarly, because DNA—which is *actually* a feature of our anatomy—reveals voluminous information about who we are, affording a third party relatively unconstrained access to it amounts to a similar affront.

One might argue that these harms are all eliminated or at least mitigated by GEDmatch's terms of service policy update (for users of GEDmatch at least), but it is not hard to imagine that even those who affirmatively opt in to allowing law enforcement access to their genetic profile do not have a full picture of what a potential investigation would actually be like, or what it could reveal. It is certainly true that the more explicit the consent is the better, but this does not eliminate the potential harms that leads may have to endure. Moreover, law enforcement may simply ignore a person's profile status even if they have not opted in. Law enforcement previously, in the GSK case, covertly uploaded the GSK's DNA pretending to be a normal user. Here too, law enforcement could employ the exact same tactic to easily bypass the thin blockade set up by a user's decision not to opt in—the harm could then be magnified if law enforcement were willing to use GEDmatch for many different crimes as they are now permitted to do.

In *Carpenter,* the majority suggests that it is extremely difficult and burdensome to live without a cell phone, and asking one to choose to opt out of purchasing a cell phone to avoid a search that effectively yields after-the-fact surveillance is akin to no choice at all.[93] Although using genetic databases is not yet "indispensable to participation in modern

---

[91] *Carpenter*, 138 S. Ct. at 2218 (quoting *Riley*, 573 U.S. at 385).

[92] *Id.*

[93] *Id.* at 2210 ("[C]ell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society.").

society," they are becoming more sophisticated, pervasive and have begun providing greater benefits, such as precision health care.[94] In particularized cases, the genetic search might be much more important to individuals than a cell phone, since these searches touch on heritage, parentage, health, and other essential aspects of life and identity. If the practice of genetic searching continues to proliferate, and especially if searches are used in concert with personalized precision medicine that requires genetic information be uploaded to a database, providing genetic information may become an essential and widespread part of people's lives.[95] Additionally, we might think that requiring someone to opt out of even a marginally useful technology lest they face potential government surveillance to be an unfair choice to impose on an innocent individual.

B. Innocent Relatives Outside the Database

Relatives of the databased person who are implicated in the investigation by virtue of their relatedness incur a separate harm. These individuals never relinquished their genetic information to a database and likely took no affirmative steps to reveal their identities. In fact, many of them may be actively trying to live a private life. Yet, in the case of DTC databases, unlike for the databased persons, there is no opt out. Even if their relatives are okay with their genetic information being examined, these individuals are never given that choice. The government is able to learn a significant amount of information about them through familial matches enabled by their relatives' decisions to upload their DNA. Once genetic information is run through a database and law enforcement determines who on the database is related to the suspect, investigators build family trees from those relatives. Nearly everyone on those trees is initially a suspect. Some of them can be easily eliminated, some of them cannot. Suspicion may be heightened and prolonged if a relative matches the suspected perpetrator's profile in some other way—and further protracted if the government does not have more promising leads.[96]

Yet relatives have the same privacy rights as individuals not

---

[94] See *id.*; Jessica Kent, *FDA Recognizes Genomic Database to Advance Precision Medicine*, HEALTH IT ANALYTICS (Dec. 7, 2018), https://healthitanalytics.com/news/fda-recognizes-genomic-database-to-advance-precision-medicine.

[95] CLN Stat, *The Rise of Personalized Medicine*, AACC (June 16, 2018), https://www.aacc.org/publications/cln/cln-stat/2016/june/16/the-rise-of-personalized-medicine ("The personalized medicine revolution is no longer coming. It has arrived.").

[96] *See, e.g.*, Bucholtz, *supra* note 86 (describing the investigation of an Oregon man who matched a specific genetic marker with GSK).

related to a databased person do, both in not being considered suspects solely on the basis of "genetic probabilities" and in maintaining privacy in their genetic information.[97] In her article *Relative Doubt,* Erin Murphy outlines the harm of investigating a databased person's kin:

> The potential harm to relatives exceeds that of even the actual offenders . . . . The relative is not just in the database once with a precise profile, but instead is in the database *multiple times* with every possible profile permutation that completes the blanks of a partial match. If familial searching is to be allowed, a relative would be wise to volunteer a genetic sample (and thus be more readily excluded) rather than run the risk of repeated requests for samples that ultimately prove not to match.[98]

While Professor Murphy refers to searching CODIS and not to a commercial database, the same concerns apply and perhaps even more strongly when law enforcement accesses genetic information in a purely private and personal context that never involves the government at inception. The choice to remain private can be taken away from a large and growing number of minimally related individuals.

Moreover, familial searches render only inexact possibilities.[99] Thus, when investigators run a familial search and consider relatives of the databased individual, the list of suspects includes mostly, possibly only, innocent individuals, and these innocent matches can number in the thousands.[100] Subjected to investigation, these individuals' lives and relationships with family members may be upended. In fact, it is entirely possible that someone in the family was the victim of the offender. In 2008, for instance, roughly two-thirds of all violent crimes occurred between non-strangers.[101] In such cases, the "suspicion cast on the relative as a result of the estranged offender can be especially painful."[102] Whether this can be justified in the case of a successful conviction depends on the extent of the damage, but in the case of no conviction, it seems harder to

---

[97] Murphy, *Relative Doubt*, *supra* note 53, at 317 (lamenting that law enforcement justifies the use of "databases to generate suspect pools, and that any follow-up investigation is not unconstitutionally suspicionless because some degree of allelic similarity makes it conceivable that an individual is the source").

[98] *Id.*

[99] Rori V. Rohlfs et al., *The Influence of Relatives on the Efficiency and Error Rate of Familial Searching*, 8 PLOS ONE (2013).

[100] *See* Hoglund-Shen, *supra* note 83, at 474.

[101] KATE M. MCQUADE, *Victim–Offender Relationship*, *in* THE ENCYCLOPEDIA OF CRIMINOLOGY AND CRIMINAL JUSTICE (Jay S. Albanese ed., 1st ed. 2014).

[102] Murphy, *Relative Doubt*, *supra* note 53, at 320.

justify.

The number of individuals potentially cast under suspicion is likely to increase since law enforcement is no longer restricted to using GEDmatch solely when solving murder and sexual assault crimes. In fact, given the breadth of the kinds of crimes now permitted, including non-negligent manslaughter, robbery, and aggravated assault, the frequency of GEDmatch searches and thus relatives who might be subjected to investigation may rise by a significant factor.

Another potential harm is misidentification. In 2014, investigators working on a two decades-old murder case in Idaho searched the public DNA database, Ancestry.com. They found 34 out of 35 markers of the Usry family—strong evidence that the DNA taken from the crime scene belonged to a member of the family.[103] In particular, the DNA seemed likely to belong to the father of Michael Usry Jr., a filmmaker in New Orleans who had, years earlier, donated a DNA sample to a genealogy project through his Mormon church in Mississippi.[104] That project's database was later purchased by Ancestry.com, making it publicly searchable.[105] Usry Jr. is a filmmaker with a short film about murder called "Murderabilia."[106] Given the subject of Usry's film, along with the fact he had been through Idaho at one point in his life, police thought they had their man.[107] As a result of the familial match and this information, Michael Usry was arrested, interrogated and "endured 33 anxiety-filled days [in police custody] until investigators realized they had the wrong person and cleared him."[108] The risk of error is another example of how cold hits stemming from familial matches can have harmful consequences for those swept up in the process.

There are psychological effects that can exacerbate the likelihood of such harms. Cold cases can be frustrating because of the amount of work that has likely been expended in the investigation and the lack of

---

[103] Jim Mustian, *New Orleans Filmmaker Cleared in Cold-Case Murder; False Positive Highlights Limitations of Familial DNA Searching*, NEW ORLEANS ADVOCATE (Mar. 12, 2015, 7:20 AM), https://www.theadvocate.com/new_orleans/news/article_1b3a3f96-d574-59e0-9c6a-c3c7c0d2f166.html.

[104] *Id.*

[105] *Id.*

[106] *Id.*

[107] *Id.*

[108] Lars Trautman & Nila Bala, *Golden State Killer Case Ushers in New Era of Fourth-Party Consent*, BROOKINGS (Jul. 3, 2018), https://www.brookings.edu/blog/techtank/2018/07/03/golden-state-killer-case-ushers-in-new-era-of-fourth-party-consent/.

results to reflect that effort.[109] Such frustration may lead investigators who now through technological improvements have leads for the first time in a long time, to view innocuous facts as inculpatory evidence against the suspect. This is a form of confirmation bias that is well-established in forensic science.[110] Professor Andrea Roth notes for example, that Brandon Mayfield, an Oregon attorney, was falsely accused of perpetrating the 2004 Madrid train bombings based only on a cold hit from the FBI's fingerprint database: "investigators found no other evidence linking him to the crime but viewed Mayfield's conversion to Islam, as well as records showing that Mayfield had left the country, as suspicious."[111]

The clouds of suspicion these innocent individuals live in are dark and noxious. Some commentators have said that the protracted suspicion engendered by these investigations could be the "worst indignity" of them all.[112] Even suspicion that is quickly dispelled can be damaging—and more so if the crime of which the individual is accused is rape or murder.[113] It has the potential to destroy careers, ruin marriages, and forever stigmatize the suspects even if they are ultimately exonerated. There is no remedy for many of these harms. Consider, for example, the kind of harms incurred by the Central Park Five who were falsely accused of murder and rape, individuals who spent years in prison and on whom a future President of the United States wanted to impose the death penalty, or the Duke Lacrosse players and University of Virginia fraternity members who were falsely accused of rape, or Stephen Hatfill who was misidentified as the anthrax mailer many years ago.[114]

---

[109] The GSK case, for instance, went on for decades.

[110] *See, e.g.*, Murphy, *Relative Doubt*, *supra* note 53, at 310; COMM. ON IDENTIFYING THE NEEDS OF THE FORENSIC SCI. CMTY., NAT'L RESEARCH COUNCIL, STRENGTHENING FORENSIC SCIENCE IN THE UNITED STATES: A PATH FORWARD (2009); David L. Faigman, *Anecdotal Forensics, Phrenology, and Other Abject Lessons from the History of Science*, 59 HASTINGS L.J. 979, 989 (2008) ("[A]necdotal forensics may be particularly susceptible to confirmation bias."); Paul C. Giannelli, *Wrongful Convictions and Forensic Science: The Need to Regulate Crime Labs*, 86 N.C. L. REV. 163, 204 (2007).

[111] Andrea Roth, *Database-Driven Investigations: The Promise—and Peril—of Using Forensics to Solve "No-Suspect" Cases*, 9 CRIMINOLOGY & PUB. POL'Y 421, 422 ("[O]thers have expressed concern that the use of forensic science to identify suspects in the first instance will supplant traditional investigatory techniques because database searches are quicker and cheaper than gumshoe detective work.").

[112] Murphy, *Relative Doubt*, *supra* note 53, at 314.

[113] *Id.*

[114] *Id.* (noting the harm caused by three out of five of those examples); *see also* Michael Wilson, *Trump Draws Criticism for Ad He Ran After Jogger Attack*, N.Y TIMES (Oct. 23,

In essence, there are many circumstances in which one would not want genetic connections to be revealed, but with the influx of DTC databases and law enforcement's increasing exploitation of those databases, one may not have that choice anymore. The decision of whether or not to be an identifiable member of the digital genetic marketplace is no longer one that people can make for themselves.

C. The Source/False Matches

A third harm is inflicted on individuals who are falsely identified through database matching as a result of a scientific mishap. Matching DNA markers against large databases can lead to misleading results because many specific markers can be shared by large portions of the population.[115] As a result, different individuals can share genetic markers with one another, which causes confusion.

Prior to GSK's identification, a false positive match led investigators to an innocent 73-year-old man residing in a nursing home in Oregon who shared a rare genetic marker with GSK.[116] Investigators first identified the genetic marker in the man's daughter (who had uploaded her DNA to a database) and then built a family tree stemming from her, which led them to her father.[117] After being put under the pressure and strain of investigation, the judge ordered him to provide DNA samples that eventually refuted the familial match, and finally cleared his name.[118]

This type of false positive presents a severe technological problem. DNA tests used by direct-to-consumer genealogy sites are less accurate than those used in forensic science even if they are often thought

2002), https://www.nytimes.com/2002/10/23/nyregion/trump-draws-criticism-for-ad-he-ran-after-jogger-attack.html; Sabrina Erdely, *A Rape on Campus*, ROLLING STONE (Nov. 19, 2014) (now withdrawn) (blaming the Phi Kappa Psi fraternity at the University of Virginia for the sexual assault of another student, later discovered to be false).

[115] *See* Erin Murphy, *The Dark Side of DNA Databases*, THE ATLANTIC (Oct. 8, 2015), https://www.theatlantic.com/science/archive/2015/10/the-dark-side-of-dna-databases/408709/ (noting that in "the Arizona database [which] had only 65,493 people in it . . . 122 sets of people shared the same genetic markers").

[116] Michael Balsamo et al., *Police Using Genetic Sites Misidentified Oregon Man as Golden State Serial Killer Suspect in 2017*, CHICAGO TRIBUNE (Apr. 28, 2018, 9:39 AM), https://www.chicagotribune.com/news/nationworld/ct-genealogy-site-serial-killer-20180427-story.html.

[117] *Id.*

[118] *Id.*

of as being similarly precise.[119] In fact, because familial DNA searching is necessarily a "scattershot approach", experts have expressed worries that investigators' use of the sites could result in "a high rate of false positives" and people being mistakenly identified as suspects.[120] In the United Kingdom, for example, a 2014 study found that just 17 percent of familial DNA searches "resulted in the identification of a relative of the true offender."[121] Yet, untrained legal professionals and jurors in criminal trials may not know the difference in accuracy.

Moreover, a familial search may often lead to the person who is the source of genetic material left at a crime scene where it turns out that person is not actually the perpetrator of the crime. At times it may be obvious that the source cannot be the perpetrator "such as the case of the man whose DNA was found on a rape-murder victim, but who was four years old at the time of the offense".[122] Other times the impossibility of the DNA match may not be so obvious. Professor Murphy notes the consequences of this: "it is also possible that, in a number of cases, identification of the source may start the investigation for corroborating evidence. And for innocent suspects without ironclad defenses, or those against whom charges are brought decades after the offense, that process raises the risks of overreliance and confirmation bias."[123] An additional harm of familial searches is that they may expose information that would otherwise remain private by divulging subjects' presence at crime scenes when they did not want their presence to be known for reasons of safety or privacy. Law enforcement cannot be faulted for testing DNA obtained at the crime scene from individuals other than the perpetrator; however, the shift towards increased reliance on commercial databases implicates new privacy concerns that must be explicitly and intentionally addressed.

---

[119] Brendan Koerner, *Your Relative's DNA Could Turn You into a Suspect*, WIRED (Oct. 13, 2015, 6:45 AM), https://www.wired.com/2015/10/familial-dna-evidence-turns-innocent-people-into-crime-suspects/ (citing U.K. study showing inaccuracy of DTC databases). It is unclear the extent to which accuracy has improved since this study was published.

[120] *Id.*

[121] *Id.*

[122] Murphy, *Relative Doubt*, *supra* note 53, at 319. This may be aggravated by recent revelations that DNA samples are becoming easier to come by, as, for example, geneticists are now able to identify individuals merely by a strand of their hair. *See, e.g.*, Heather Murphy, *Why This Scientist Keeps Receiving Packages of Serial Killers' Hair*, N.Y. TIMES (Sept. 16, 2019), https://www.nytimes.com/2019/09/16/science/hair-dna-murder.html.

[123] *Id.*

D. Potential Harms of Genetic Searching

If genetic searching remains a free-for-all without judicial oversight or regulation people can justifiably fear that private entities such as insurance companies will gain access to the databases. Many civil rights and medical organizations have expressed concern that DTC databases will lead to individuals being denied coverage based on their genotype and findings from stored samples.[124] Although these current databases primarily serve personal purposes and law enforcement, it is conceivable that information may be widely shared or even sold in the future and possibly used as a form of genetic discrimination. Moreover, one might worry that the genetic information obtained by law enforcement could somehow make its way into the hands of insurance providers who could, in some future healthcare scheme without the Genetic Information Nondiscrimination Act of 2008, deny or discriminately price insurance to reflect an individual's propensity for certain illnesses or disorders.[125] One could also envision advertisers employing widespread gene-based marketing where if you carry the genetic variants associated with certain traits, advertisers market products that suit that trait.[126] For instance, someone with genetic markers for lactose intolerance may see more Lactaid advertisements, or someone with genes for male-pattern baldness may see advertisements for Rogaine.[127]

Genetic discrimination is already a reality in other countries. Genetic material is currently a critical part of China's campaign to identify Chinese persons of Uighur descent—a Turkic ethnic group who live in East and Central Asia and generally practice Islam—and force them into camps as part of a nationwide "re-education campaign."[128] China is using genetic tools, including information obtained from commercial databases to "chase down any Uighurs who resist conforming

---

[124] *See, e.g.*, Paul R. Billings et al.*, Discrimination as a Consequence of Genetic Testing*, 50 AM. J. HUM. GENET. 476 (1992); LORI B. ANDREWS ET AL., ASSESSING GENETIC RISKS: IMPLICATIONS FOR HEALTH AND SOCIAL POLICY (1994).

[125] *See generally* Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881 (2008).

[126] Susan Young Rojahn, *Marketing to the Big Data Inside Us*, MIT TECH. REV. (2013).

[127] *Id.*

[128] Sui-Lee Wee, *China Uses DNA to Track Its People, With the Help of American Expertise*, N.Y. TIMES (Feb. 21, 2019), https://www.nytimes.com/2019/02/21/business/china-xinjiang-uighur-dna-thermo-fisher.html.

to the campaign."[129] Chinese scientists have contributed DNA samples from individuals of Uighur descent to identify their relatives.[130] These officials also tout the crime-fighting benefits of the technology, looking in part at the successes of DTC databases in the United States. [131]

This may become a more severe issue given that the firewall between CODIS STR profiles and DTC database SNP profiles is not as strong as once thought, and a CODIS profile, ostensibly lacking identifying information such as genes for eye color or a disease, can now essentially be converted to an SNP profile, which may contain such identifying information.[132]

Furthermore, now that GEDmatch has expanded the list of crimes for which it is willing to grant access to law enforcement, there is a real concern echoed by geneticists that GEDmatch and similar companies will continue to expand this list to crimes of lesser and lesser severity. This means that individuals will likely be caught in the dragnet, and the government's surveillance power will further expand.

Finally, despite the updates to the terms of service of GEDmatch, one might worry that law enforcement could simply circumvent a user's decision to opt out of providing law enforcement access to their profile. In the first instance, as mentioned above, law enforcement covertly uploaded the GSK's DNA while pretending to be a normal user. Law enforcement could once again pretend to be a normal user at which point a judge—assuming a suppression motion were even made—would have to decide if this use of GEDmatch is improper such that any evidence recovered should be excluded.

All of these harms should be considered when conducting a legal analysis of the issue. Part IV examines whether the Fourth Amendment provides any protection for the harms that a government-initiated genetic database search may inflict on these parties.

IV. FOURTH AMENDMENT ANALYSIS

A threshold question before any form of balancing is whether a search actually takes place. As described in Part III, there are three distinct types of individuals (all relevant in the GSK investigation and arrest) on whom some form of a search is conducted and who—in different ways—

---

[129] *Id.*
[130] *Id.*
[131] *Id.*
[132] *See* Molteni, *Genome Hackers*, *supra* note 54.

either directly or indirectly and voluntarily or involuntarily, contribute their genetic information in service of the investigation: (1) the databased persons; (2) the databased persons' relatives; and (3) the source(s) of genetic information left at the crime scene. The following section focuses on the first two categories where the unsettled questions of law lie.

In his concurring opinion in *Katz v. United States*, Justice Harlan established a two-pronged test eventually adopted by the Supreme Court to determine when a government search is subject to the Fourth Amendment: "first that a person have [sic] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[133] To meet the first prong, the person subject to the search must prove that they had an actual subjective expectation that the fruits of the search would not normally be available to the public.[134] The second prong is analyzed objectively by examining whether society would generally deem the individual's expectation of privacy to be reasonable. If it is obvious that an individual did not keep evidence private, then no search subject to the Fourth Amendment is required to uncover the evidence. Examples of places where one might have a reasonable expectation of privacy are a person's home, hotel room, car, or private portions of jailhouses.[135] As a general matter, items left in plain view, abandoned, or put out to the public—for example, garbage taken out of the home and placed at the curb—are not afforded protection because one does not have a reasonable expectation of privacy in them.[136]

A. Searches of Databased Persons

Most of the jurisprudence regarding DNA searches focuses on the moment when a DNA sample is collected from the crime scene or from the individual separately.[137] The general consensus thus far has been that an invasion of a subject's privacy ends once the initial DNA is extracted.[138] The assumption has been that any subsequent examination of that DNA is merely a reexamination of already-acquired information

[133] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
[134] *Id.*
[135] PAUL BERGMAN & SARA BERMAN-BARRETT, THE CRIMINAL LAW HANDBOOK: KNOW YOUR RIGHTS, SURVIVE THE SYSTEM (2007).
[136] *See, e.g.*, California v. Greenwood, 486 U.S. 35, 43–44 (1988) (holding that no search occurs when police look through someone's garbage).
[137] *See* Erin Murphy, *Paradigms of Restraint*, 57 DUKE L.J. 1321, 1329–30 (2008).
[138] *See* Murphy, *Relative Doubt*, *supra* note 53, at 333.

and reveals no "new, private or intimate information," and as such, does not create a new Fourth Amendment issue.[139]

The process of finding matches within a database has generally been ruled constitutional. In an opinion that was subsequently vacated after a guilty plea was entered, the U.S. Court of Appeals for the Ninth Circuit stated that, "it is not clear that familial comparisons raise a constitutional privacy issue or, if they do, whose interests are violated."[140] In *Nicholas v. Goord*, the U.S. Court of Appeals for the Second Circuit recognized the potential harm of DNA databases based on the fact that DNA can be stored indefinitely. Although the court acknowledged that DNA databases pose "potentially a far greater intrusion than the initial extraction of DNA, since the state analyzes DNA for information and maintains DNA records indefinitely," it nevertheless found the procedural safeguards in New York sufficient to allay the court's concerns.[141]

Even the few courts that have acknowledged constitutional claims based on genetic profile searching have not examined the subsequent genetic search process as a separate matter from the initial DNA acquisition.[142]

Still, courts have not considered the question of DTC databases yet. Up until this year, the most prominent genealogy databases for law enforcement had a system of implied consent to law enforcement's access. GEDmatch—perhaps the most prominent of all databases with regard to law enforcement—has shifted their method of obtaining consent from a general advisory to an affirmative opt-in process. Under both systems, potential Fourth Amendment issues abound.

Time and again courts have emphasized that arrestees relinquish their right to privacy by virtue of their alleged crimes.[143]

---

[139] Boroian v. Mueller, 616 F.3d 60, 67 (1st Cir. 2010).

[140] United States v. Pool, 621 F.3d 1213, 1221 (9th Cir. 2010) ("It is questionable whether the rights of the perpetrator (if ultimately identified through the use of familial comparisons) are violated.")

[141] 430 F.3d 652, 670 (2d Cir. 2005) ("New York statute as written does not provide for sensitive information to be analyzed or kept in its database. Rather, it provides only for the analysis of identifying markers." (citing N.Y. Exec. Law § 995-c(3), (5))).

[142] *See* Murphy, *Relative Doubt*, *supra* note 53, at 333; *see also* United States v. Weikert, 504 F.3d 1, 13, 5–17 (1st Cir. 2007) (failing to distinguish the separate potential privacy intrusion that occurs when observing a genetic profile as opposed to mere sample acquisition required to create the profile).

[143] *See, e.g.*, Maryland v. King, 569 U.S. 435, 463 (2013); Florence v. Bd. of Chosen Freeholders, 566 U.S. 318 (2012).

Previous rulings have been predicated on this fact and therefore the viewing of their (supposedly less revealing) genetic profile in CODIS is justifiable.[144] However, databased individuals in DTC databases present a new legal context in which different and likely stronger privacy rights are implicated. Moreover, at least in certain states, courts have begun to acknowledge that there are separate Fourth Amendment issues between the DNA collection phase and the creation of a profile and analysis phase.[145]

Nationally, as noted above, the Supreme Court has begun to refine the boundaries of the Fourth Amendment in the face of new technologies, even if the result is doctrinally challenging and undeveloped. This process of doctrinal fine-tuning has been called "equilibrium adjustment" whereby "the Supreme Court adjusts the scope of Fourth Amendment protection in response to new facts in order to restore the status quo level of protection. When changing technology or social practice expands government power, the Supreme Court tightens Fourth Amendment protection . . . ."[146] This theory has been used convincingly to explain a "wide range of puzzling Fourth Amendment doctrines, including the automobile exception; rules on using sense-enhancing devices . . . how the Fourth Amendment applies to the telephone network; undercover investigations [etc.]"[147] as well as the cell-site location information in *Carpenter*.[148] It is reasonable to believe that, as with these other technologies, the harms of the forensic use of DTC databases are great enough to warrant a finding that the government must step in to regulate the technology and prevent these harms. This has been suggested about *Carpenter*, where "a search occurred because it needed to have occurred to regulate a practice that needed to be regulated to keep the government from having too much power."[149]

---

[144] *King*, 569 U.S. at 463.

[145] *See, e.g.*, People v. Buza, 180 Cal. Rptr. 3d 753, 762–63 (Ct. App. 2014) ("The collection of the DNA sample, however, is only the first part of the search . . . the second occurs when the DNA sample is analyzed and a profile created for use in state and federal DNA databases."), *rev'd*, 413 P.3d 1132 (Cal. 2018).

[146] Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011) [hereinafter Kerr, *Equilibrium-Adjustment Theory*].

[147] *Id.*

[148] Orin Kerr, *When Does a Carpenter Search Start—and When Does It Stop*, LAWFARE (July 6, 2018, 10:24 AM), https://www.lawfareblog.com/when-does-carpenter-search-start-and-when-does-it-stop [hereinafter Kerr, *Carpenter Search*].

[149] *Id.*

Additionally, *United States v. Maynard* supports the proposition that people may have a reasonable expectation of privacy in their aggregate information, because the government can use the aggregate, if not the individual components, to piece together a complete picture of someone's life.[150] This "mosaic theory"—also discussed in *Jones*—established that a set of "nonsearches aggregated together amount to a search because their collection and subsequent analysis creates a revealing mosaic" of a person.[151] As genetic sequencing technology advances, and law enforcement can learn more and more about a person from their DNA, forensic use of DTC databases could constitute a search either under an equilibrium-adjustment or mosaic theory.

1. Does the third-party doctrine obviate the government's need to obtain a warrant?

If the Court finds there to be a search involved at the outset, it still must grapple with whether genetic profiles are material covered by the third-party doctrine. If the genetic profiles are covered, it would allow the government to avoid the need for a warrant by recognizing that a person has given consent by uploading their genetic information to a third party.[152]

As discussed in *Katz v. United States*, because certain information shared with the public is not protected by the Fourth Amendment, law enforcement can gain access to those records without the need for a warrant.[153] While the ultimate holding of *Katz* was to protect certain Fourth Amendment rights, this concept of the surrender of privacy later broadly foreclosed protection of information exposed to third parties.[154] The justification—codified in subsequent Supreme Court cases—is that individuals, by disclosing their information to a third party, have forfeited their Fourth Amendment rights in those

[150] United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) (ruling that the warrantless use of a GPS tracking device place on a car is unconstitutional).

[151] Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 320 (2012) [hereinafter Kerr, *Mosaic Theory*]; United States v. Jones, 565 U.S. 400, 412 (2012).

[152] *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2263 (2018).

[153] 389 U.S. 347, 351 (1967); *see also* Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 443 (1976).

[154] *See generally Katz*, 389 U.S. 347; *see also* Smith, 442 U.S. at 743–44; Miller, 425 U.S. at 443.

records. The doctrine has expanded significantly as technology has advanced.[155]

A series of third-party doctrine cases involving various kinds of business records followed *Katz* from 1973 to 1980. In each one of these cases, the Court ruled that transferring business records to third parties relinquished Fourth Amendment protection. In *Smith v. Maryland*, the Court applied the third-party doctrine to pen registers—a device installed at the phone company to record the numbers dialed from a specific telephone.[156] In *Smith*, investigators requested that a phone company install a pen register on the home phone of a man who was suspected of robbing and then harassing a woman by making repeated anonymous phone calls.[157] The Supreme Court held that this use of a pen register was not a Fourth Amendment search because it was covered under the third-party doctrine, and that the defendant had "assumed the risk" by using his phone.[158]

Despite the centrality of a telephone to a person's life, the Court at that time had little trouble dismissing the notion of any privacy interest in the numbers dialed since the records were with the phone company. But after many decades the tide is turning on that mechanical analysis.[159]

In *United States v. Jones*, the Supreme Court unanimously held that "around-the-clock tracking of a personal vehicle for weeks, accomplished by placing a magnetized GPS tracker to the underside of the car" was a search that violated the Fourth Amendment.[160] The Court showed fissures forming in the third-party doctrine in the Justices' various opinions, which reflected anxiety over how well the doctrine fit with evolving technologies. First, the Court was sharply

---

[155] *See, e.g.*, *Carpenter*, 138 S. Ct. at 2219 (describing how cell-site location information could not have been anticipated as a use of the third-party doctrine when it was developed).

[156] 442 U.S. 735.

[157] *Id.* at 742.

[158] *Id.* at 745; 18 U.S.C. § 3121. A pen register, at least in federal practice, requires an order that is signed by a judge, providing some minimal judicial oversight—more than that which is available for genetic databases.

[159] *See Katz*, 389 U.S. at 750; *Smith*, 442 U.S. at 749, 751 (Marshall, J., dissenting) ("The prospect of unregulated government monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide.").

[160] David H. Kaye, *The Genealogy Detectives: A Constitutional Analysis of "Familial Searching,"* 50 AM. CRIM. L. REV. 109, 133 (2013) (summarizing the holding of *Jones*).

divided on how to treat the GPS tracking.[161] Second was a recognition by the Court that technology had, at least in this instance, outgrown traditional doctrines that were now insufficient for the digital era.[162] Justice Sotomayor noted her discomfort with the third-party doctrine:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks . . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[163]

Justice Sotomayor also reaffirmed the force of the mosaic theory mentioned above which, by "aggregating conduct rather than looking to discrete steps, . . . offers a fundamental challenge to current Fourth Amendment law."[164]

The Court exhibited continued skepticism about the adequacy of existing privacy regimes in the face of rapidly developing, expansive and intrusive technologies upon which people now rely. The concern was expressed in *Riley v. California*. In that case, David Riley, a gang member in San Diego, was pulled over, and had his car impounded and searched.[165] The police found two guns in his car, arrested Riley for possession of firearms and searched his cell phone which contained evidence tying Riley to a shooting.[166] The Supreme Court ruled that this warrantless search was unlawful because cell phones hold "for many Americans 'the privacies of life.'"[167]

Four years later, the Court decided *Carpenter v. United States*, a case involving an April 2011 incident in which police arrested four men in connection to a series of robberies.[168] One of the men confessed

---

[161] United States v. Jones, 565 U.S. 400, 406 (2012) ("[F]or most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas . . . it enumerates. *Katz* did not repudiate that understanding."); Kaye, *supra* note 160, at 408 n.5 ("Trespass . . . conjoined with . . . an attempt to find something or to obtain information" should be considered a search.).

[162] *Id.* at 417–19.

[163] *Id.* at 417–18.

[164] Kerr, *Mosaic Theory*, *supra* note 151, at 314.

[165] Riley v. California, 573 U.S. 373, 378 (2014).

[166] *Id.*

[167] *Id.* at 403 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

[168] 138 S. Ct. 2206, 2212 (2018).

to his involvement in the crimes and provided the FBI his cell phone number and the numbers of the other perpetrators.[169] The FBI used this information to obtain seven days of transaction records for each of the numbers, including the time of calls made and received as well as the approximate location where those calls began and ended based on which cell tower was closest at the time.[170] This latter kind of information is known as cell site location information (CSLI). Based on this evidence, the government charged Timothy Carpenter with "six counts of robbery and an additional six counts of carrying a firearm during a federal crime of violence."[171]

The Supreme Court held that the government's warrantless acquisition of the historical CSLI records was an unconstitutional search.[172] The majority emphasized that the expectations of privacy in the 21st century do not fit neatly into existing privacy doctrine, and that tracking one's location with CSLI records was a far more intrusive practice than the third-party doctrine was envisioned to allow.[173] Moreover, the third-party doctrine is supposed to apply only to voluntary exposure—which was not exactly the case in *Carpenter.*[174] The Court held that while a user might be abstractly aware that her cell phone provider maintains logs of her calls, it happens without any real affirmative action aside from powering the cell phone.[175] The finding that a search occurred reflected the Court's discomfort with technology that was too expansive and intrusive in its view, and a consent that was questionable.

The Court held narrowly that, even with user consent, where technology had intruded within the bounds of reasonable expectations of privacy, the government is required to obtain a warrant.[176] The Court left further questions about the parameters of the third-party doctrine unclear, especially as applied to other expansive technologies that do not fit well into existing precedent.[177]

---

169 *Id.*
170 *Id.* at 2212.
171 *Id.*
172 *Id.* at 2223.
173 *Id.* at 2220.
174 *Id.*
175 *Id.*
176 *Id.*
177 *Id.* (clarifying that this decision does not address matters not before the Court and does "not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor [does it] address other

A principal premise of *Carpenter* is that, in the past, when much of the orthodox privacy doctrine originated, the public would not have expected the government to be able to track the location of a subject so comprehensively, furtively, and easily. As Chief Justice Roberts writes for the majority, "Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so for any extended period of time was difficult and costly and therefore rarely undertaken."[178] Quoting Justice Alito's concurrence in *Jones*, Roberts noted "law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[179] The use of "in the main" masks a conceptual weakness because in fact the government could do what Chief Justice Roberts says it could not. Law enforcement *could* have a team of agents tailing a suspect at all times and perhaps that did occur in the 1950s and 60s. But, as a practical matter, in nearly all cases this level of surveillance had not been undertaken, and if it were, it could not continue for long due to resource constraints.[180] Even though the decision was narrow, the principle is clear: technology has outgrown traditional privacy doctrine, and the Court, recognizing this, is beginning to step in to counterbalance the harms this mismatch engenders.

Carpenter is an example of equilibrium adjustment in which "technology dramatically expand[ed] the government's power under an old legal rule, . . . [so] the Court change[d] the legal rule to restore the prior level of government power."[181] The fact that the surveillance is "detailed, encyclopedic, and effortlessly compiled" and "provides an all-encompassing record of the holder's whereabouts" is too intrusive to be permitted.[182] The third-party doctrine was, in part, developed based on the "nature of the particular documents sought," which were limited in the information they could yield.[183] CSLI data are far more intrusive than are the phone records of years ago, or bank records, and

business records that might incidentally reveal location information . . . does not consider other collection techniques involving foreign affairs or national security").

[178] *Id.* at 2217 (internal quotations and citation omitted).

[179] *Id.*

[180] Therefore, creating full surveillance through records like CSLI is extremely powerful and difficult to replicate. *See generally* Kerr *Carpenter Search*, *supra* note 136.

[181] *Id.*

[182] *Carpenter,* 138 U.S. at 2209, 2217.

[183] *Id.* at 2210 (citing United States v. Miller, 425 U.S. 435, 442 (1976)).

thus do not fit comfortably within the third-party doctrine. Because technology has advanced, making law enforcement's capabilities too expansive in the context of striking the privacy versus security balance, the third-party doctrine had to be constricted (or the Fourth Amendment expanded) restoring privacy to a level of reasonable expectation that individuals once had.

Carpenter, in many ways, traces a concern that could very well animate the judicial view of DTC databases. In the past, genetic database searches were constitutionally permitted based on the seemingly limited amount of information they reveal. They were supposed to be merely identifying numbers that revealed nothing else about an individual. The limited nature of genetic searches was the operative premise of *Maryland v. King* and a host of other cases.[184] Meanwhile, much of the jurisprudence surrounding genetic databases is focused on the point of acquisition of the suspect's genetic material, which has largely been held as constitutional. DTC databases turn much of this prior jurisprudence on its head in ways that echo *Carpenter*. As is now being realized, genetic databases can paint a deep picture of a person: of their health, their heritage, and many other things personal, private and of consequence. Moreover, DTC databases may not appear particularly intrusive when examined at specific points in a vacuum, but when the whole process is examined—from acquisition to investigation of the databased person's relatives—it begins to look a lot more intrusive and harmful, like a genetic dragnet. Investigative power has profoundly increased as a result of genetic databases. This kind of a development was certainly not contemplated during the time period in which the third-party doctrine was developed. Now, it could validly be considered outside the bounds of the doctrine, as the search in *Carpenter* was.

Even if the Court were to decide that DTC databases *are* within the bounds of the third-party doctrine, the specific consent given in the case of these databases may not hold up. In the absence of a warrant the "[s]tate assumes the burden of overcoming the presumption of invalidity by demonstrating . . . that the warrantless search satisfied

[184] *See, e.g.*, 569 U.S. 435, 464 (2013) (allowing genetic information to be taken from arrestees based on the purportedly non-identifying nature of the STR analysis); Johnson v. Quander, 440 F.3d 489 (D.C. Cir. 2006). For a more exhaustive list, *see* Murphy, *Law and Policy*, *supra* note 47, at 330–40.

one of the firmly established exceptions to the warrant requirement."[185] Consent is one of those exceptions.[186] The government has the burden of showing that consent was freely and voluntarily given. However, following that determination, someone who gives consent to a government search can "of course delimit as he chooses the scope of the search."[187] Thus, the government must also ensure that the search was actually within the scope of given consent.

In the context of DNA, consent can be granted to law enforcement in two ways: first, an individual can consent to any future use of their DNA or the court may determine that general consent to all future uses is implied; and second, an individual may limit the scope of a consent search to a particular breadth, investigation, or the court may find an implied limited scope.[188] The government bears the burden of demonstrating either express consent, or that the search of the DNA was within the scope of implied consent as measured by the standard of "objective reasonableness."[189]

A significant issue with DNA records, which can be retained indefinitely, is the duration of consent. For example, in *United States v. Kriesel*, a divided Ninth Circuit Court of Appeals debated the propriety of DNA retention.[190] Edward Kriesel pled guilty to drug conspiracy, agreed to submit his blood for DNA analysis, and his profile was added to CODIS.[191] Subsequently, Kriesel demanded that the government return his blood sample—arguing that the sample was

---

[185] Graham v. State, 807 A.2d 75, 87 (Md. Ct. Spec. App. 2002); *see also* Jones v. United States, 357 U.S. 493, 500 (1958).

[186] *See, e.g.*, United States v. Drayton, 536 U.S. 194 (2002) (holding that consent to a police officer's search of luggage on bus aisle obviates the warrant requirement where consent was voluntary and free from intimidation or coercive action); Schneckloth v. Bustamonte, 412 U.S. 218 (1973) (holding that consent need be voluntary, but not necessarily knowing and intelligent as in Miranda); Camara v. Mun. Court of S.F., 387 U.S. 523, 528-29 (1967) ("one governing principle, justified by history and by current experience, has consistently been followed: except in certain carefully defined classes of cases, a search of private property without proper consent is 'unreasonable' unless it has been authorized by a valid search warrant."); *see also* Stoner v. California, 376 U.S. 483 (1964); United States v. Jeffers, 342 U.S. 48 (1951); Agnello v. United States, 269 U.S. 20 (1925).

[187] Florida v. Jimeno, 500 U.S. 248, 252 (1991).

[188] Stephen Mercer & Jessica Gabel, *Shadow Dwellers: the Underregulated World of State and Local DNA Databases*, 69 N.Y.U. ANN. SURV. AM. L. 639, 663–64 (2014).

[189] *Id.* at 664; *see* State v. Binner, 886 P.2d 1056, 1059 (Or. Ct. App. 1994).

[190] 720 F.3d 1137 (9th Cir. 2013).

[191] *Id.* at 1137; 1141–42.

his property.[192]

The majority on the panel agreed with Kriesel, but decided that the government had a compelling interest in retaining it, and therefore Kriesel was not entitled to its return.[193] Still, the Ninth Circuit recognized the limits of its ruling, noting that we now live in a "rapidly changing world in which risks of undue intrusions on privacy are also changing."[194] The court further emphasized that "if scientific discoveries make clear that junk DNA [non-coding DNA] reveals more about individuals than previously understood, [the court] should reconsider the government's DNA collection programs."[195] As we now know, "junk" DNA *does* reveal more about individuals than previously understood.[196]

Moreover, the dissent put forth vigorous opposition, stressing that investigative tools like the use of genetic databases are "intended to aid in investigation, not to supplant it entirely."[197] The fact that Kriesel was subjected to "the retention, for at least the remainder of [his] lifetime, of his full genetic code," was unacceptable.[198] Noting the consequences of such indefinite retention, the dissent went on to proclaim that "[w]e do not need scientists to discover anything new to know that a full specimen of an individual's DNA reveals private information about that individual's predisposition for certain diseases and disorders, paternity and other familial relationships, and racial ancestry."[199]

If the *Kriesel* dissenters (and perhaps also the majority) were to analyze the privacy interests implicated in a case like the GSK case, they would note that similar expansive and essentially indefinite retention following a match might intrude upon reasonable expectations

---

[192] *Id.*

[193] *Id.* at 1139–40.

[194] *Id.* at 1147.

[195] *Id.*

[196] David H. Kaye, Bioethical Objections to DNA Databases for Law Enforcement: Questions and Answers, 31 SETON HALL L. REV. 936, 943 (2001) (explaining that "junk" DNA thus "produces a set of numbers that are useful for identification purposes and nothing else"); *but see* Edge, *supra* note 47 (noting that junk DNA actually can be useful for far more than mere identification).

[197] *Kriesel*, 720 F.3d at 1156 (Reinhardt, J., dissenting) ("Our criminal justice system successfully deterred and punished crime for hundreds of years before the use of DNA evidence became standard practice.").

[198] *Id.* at 1150.

[199] *Id.* at 1157.

of privacy, especially considering SNP analysis used in DTC tests reveals much more about a person than did the analysis considered in *Kriesel*.

A person who submits their DNA to a site does so for a particular and highly personal purpose—and government use is likely squarely outside that purpose. They agree to terms that the site lists in their clickwrap agreement (including providing law enforcement access to their information).[200] But, as illustrated by *Carpenter*, just because a term is agreed to in theory does not mean it will withstand scrutiny in a court of law. Thus, if a court finds that: 1) the possibility of government use of one's DNA for investigations, and the prospect of becoming a genetic informant, is not fully contemplated even if formally consented to in the agreement; and 2) genetic databases are important enough that, despite the third party consent acquired, the choice to not use one because of the wrap agreement is not a valid one to be imposed on a person, then a search might be found. If the databased person(s) who was matched in the GSK case fulfilled those two criteria, the process may have been invalid in the absence of a warrant. Whether this matters might again depend considerably on how a court would determine the strength of the clickwrap agreement consent and how severe it considers the potential privacy intrusions involved.

Even with regard to GEDmatch's new terms of service in which affirmative consent is required, there is reason to believe that the consent may not be valid. When a user opts in to law enforcement's use of their DNA, they are likely not giving consent to the full extent and duration of the search. It is unlikely the individual fully appreciates that such consent is effectively perpetual consent once an investigation is underway. Moreover, as is discussed above and will be discussed below, this consent is not only on behalf of the GEDmatch user themselves but also all of their relatives who will bear the brunt of the investigative scrutiny and who also almost certainly have not had any input regarding the user's decision to bring them to law enforcement's attention through their shared private DNA.

Therefore, the third-party doctrine does not clearly obviate the need for a warrant when it comes to genetic database searching. In the wake of *Carpenter*'s clarion concerns about rapidly advancing technology's intrusion into our privacy, the issues of what is a reasonable expectation of privacy and what is the substantive and

[200] *See* GEDmatch.com, *supra* note 20.

temporal scope of consent in the face of genetic technology are serious undecided questions the courts are bound to encounter soon.

2. If the third-party doctrine does not obviate the government's need to obtain a warrant, is it still otherwise "reasonable" for the government to conduct the search without a warrant under the Riley balancing test?

In *Vernonia School Dist. 47J v. Acton*, the Supreme Court held that "[a]s the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is 'reasonableness.'"[201] In *Riley*, the Court noted that in determining whether a search is exempt from the warrant requirement, a court should assess "the degree to which it intrudes upon an individual's privacy and . . . the degree to which it is needed for the promotion of legitimate governmental interests."[202] *Carpenter* and *United States v. Warshak* also suggest a new view that the third-party doctrine only diminishes a reasonable expectation of privacy, but does not eliminate it (as older cases suggest).[203] Thus, if the reasonable expectation of privacy is only diminished, reasonableness balancing still applies.

Counseling in favor of the forensic deployment of DTC databases is the invaluable investigative advantage they provide law enforcement.[204] As of the start of April 2019, "[Parabon Nanolabs] had assessed 209 cases, deciding that 137 of them could potentially be solved through genealogy . . . [and] has cracked 46 cases, with new ones being solved on a roughly weekly basis."[205] Many individuals are not on government databases because they have not been arrested and are thus not readily findable without alternative investigative means to

[201] 515 U.S. 646, 652 (1995).

[202] Riley v. California, 573 U.S. 373, 374 (2014) (citing Wyoming v. Houghton, 526 U. S. 295, 300 (1999)).

[203] *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018); United States v. Warshak, 631 F.3d 266, 285 (6th Cir. 2010) ("[T]rusting a letter to an intermediary does not necessarily defeat a reasonable expectation that the letter will remain private.").

[204] This capability manifests itself not only for solving crimes, but also for mere identification purposes. *See, e.g.*, Jessica Borg, *'Killing Fields' Victims Identified with Help of Houston-Based DNA Company*, KHOU11 (Apr. 15, 2019, 1:11 PM), https://www.khou.com/article/news/local/killing-fields-victims-identified-with-help-of-houston-based-dna-company/285-bf3e20ef-73fb-4075-a837-b103bbea7042.

[205] Aldhous, *supra* note 17.

do so.[206] Additionally, because familial searching is generally proscribed on government databases, the government has an interest in being able to cast a significantly wider net than it otherwise could—one that can find individuals even distantly related to the growing percentage of Americans who have decided to use DTC databases.[207]

Still, the mere fact of a technology's utility to law enforcement does not render it a reasonable intrusion on privacy, and it becomes less reasonable if law enforcement were to use these databases to solve less severe crimes.[208] Moreover, the concerns surrounding DNA databases are not present because people believe them not to be useful to law enforcement—they clearly are—but are instead raised because of the intrusiveness of the databases.

Increasingly, judges across the country have expressed concerns about DNA databases and the intrusiveness of mining those databases for different kinds of genetic information. For example, in *Patterson v. State*, an Indiana appellate court found that "[a]t a minimum, it is clear that the results of DNA analysis provide extremely personal information about an individual," even though the court subsequently upheld the constitutionality of the genetic-database statute.[209] In his concurrence in the *en banc* decision in *United States v. Kincade*, a case dealing with the constitutionality of collecting and retaining DNA from parolees, Judge Gould of the Ninth Circuit Court of Appeals expressed deep concerns about the evolving sophistication of DNA technology and its concomitant expansion:

> In our age in which databases can be 'mined' in a millisecond using super-fast computers, in which extensive information can, or potentially could, be gleaned from DNA (even the 'junk' DNA currently used), and in which this data can easily be stored and shared by governments and private parties worldwide, the threat of a loss of privacy is real, even if we cannot yet discern the full scope of the problem.[210]

---

[206] *See, e.g.*, Thomas Fuller, *How a Genealogy Site Led to the Front Door of the Golden State Killer Suspect*, N.Y. TIMES (Apr. 16, 2018), https://www.nytimes.com/2018/04/26/us/golden-state-killer.html. The GSK himself was not on government databases, otherwise law enforcement would have found him when they ran their searches on CODIS and in state databases, as mentioned above.

[207] *See* Scutti, *supra* note 60.

[208] *See, e.g.*, Molteni, *Creepy Genetics*, *supra* note 66 (noting that California's policies allow genetic searches only in the case of very severe crimes).

[209] 742 N.E.2d 4, 11 n. 3 (Ind. Ct. App. 2000).

[210] United States v. Kincade, 379 F.3d 813, 842 (9th Cir. 2004).

More dramatically, in a dissent in the same case, Judge Reinhardt wrote extensively about the dangers of CODIS to citizens' privacy:

> The DNA "fingerprint" entered into CODIS likely has the potential to reveal information about an individual's "genetic defects, predispositions to diseases, and perhaps even sexual orientation." Compared to its modest beginnings, [modern DNA searching] represents an alarming trend whereby the privacy and dignity of our citizens [are] being whittled away by imperceptible steps. Taken individually, each step may be of little consequence. But when viewed as a whole, there begins to emerge a society quite unlike any we have seen—a society in which government may intrude into the secret regions of man's life at will.[211]

Judge Reinhardt's concerns capture fears that must be taken seriously when faced with a rapidly evolving technology that, as it expands, encroaches more and more on expectations of privacy. The same alarm sounded in *Jones* and *Carpenter* is sounded by Judge Reinhardt in relation to genetic testing. It is a prescient but also present concern that must be addressed.

Finally, in *Birchfield v. North Dakota* the Court noted that blood tests are more invasive than breath tests partially because there are other types of information that can be detected using blood samples, thus requiring a warrant.[212] This echoes a fundamental concern with regard to DTC databases, as they can reveal information different in kind and degree than traditional government DNA databases were thought to reveal.

The various relatives of GSK who were matched and from whom a family tree was grown likely did not intend for their genetic information to be used in a government investigation when they initially submitted their DNA to a commercial service. Further, it is important to note that even if one has diminished her own privacy right this does not mean that the Fourth Amendment falls out of the picture entirely.[213]

Although there has not yet been a decision ruling any kind of

---

[211] *Id.* at 850–51.

[212] 136 U.S. 2160, 2165 (2016).

[213] *See* Riley v. California, 573 U.S. 373, 392 (2014) (citing Maryland v. King, 569 U.S. 435, 463 (2013)) ("[N]ot every search 'is acceptable solely because a person is in custody' . . . to the contrary, when 'privacy-related concerns are weighty enough' a 'search may require a Warrant, notwithstanding the diminished expectations of privacy of the arrestee.'").

familial searching to be a Fourth Amendment search, it is clear that judges view the expansion and increased sophistication of these databases with apprehension. Courts have not yet had to confront questions involving a DTC database as opposed to a government one. A voluntary DTC database that is designed to answer important personal concerns about family, origins, health, and other sensitive elements of one's identity, and which leads to other individuals in and outside the database is even more alarming in terms of its implications for privacy than are the concerns identified by Judge Reinhardt about CODIS. This is especially true because DTC databases allow law enforcement to bypass the stricter regulations imposed on government databases. The fact that in *Birchfield* a blood test explicitly *required* a warrant because of many of the same concerns present with regard to DTC databases (namely, how revealing the information can be) suggests that the Court may find the forensic application of consumer genetics without a warrant to be unreasonable. This is especially true considering *Rise v. Oregon*, in which the Ninth Circuit Court of Appeals held that "DNA genetic pattern analysis is even more intrusive than [a] blood alcohol test."[214]

B. Searches of Relatives of Databased Persons

In the reasonableness analysis, the effects on others who never made any affirmative act that could have led to their diminished privacy expectations should also be an integral part of the equation. It is with regard to these individuals that the search is most expansive and the greatest number of people are implicated, as investigators can indiscriminately surf through a vast number of often minimally connected individuals based on their kin's genetic profile. In the GSK case, investigators spent four months building out family trees, name by name, based on matches uncovered when searching GEDmatch. The investigators then followed up on individuals included in those trees.[215] Detective Paul Holes, the lead investigator in the case, explained how wide a nest they cast saying "we are talking third, fourth and fifth cousins and more distant than that."[216] The average person

[214] 59 F.3d 1556, 1564 (9th Cir. 1995).

[215] *See* Jouvenal, *supra* note 13.

[216] Richard Winton, et al., *The First Step in Finding Golden State Killer Suspect: Finding His Great-Great-Great-Grandparents on Genealogy Site*, L.A. TIMES (Apr. 27, 2018, 5:10 PM), https://www.latimes.com/local/lanow/la-me-golden-state-dna-match-20180427-story.html.

has around 4,700 fifth cousins.[217] Not all of the individuals identified were actually on GEDmatch, but they were identifiable to police through their relation to individuals who *were* on GEDmatch. Ultimately, one of these relatives was DeAngelo himself. Such a practice might be considered more invasive than that addressed in *Carpenter,* where the government was collecting information on *known* individuals. With a genetic database search the databased individual's self-inflicted diminished privacy should not, as a matter of principle, also be permitted to diminish the privacy of her relatives, an intrusion that is magnified because of the sheer number of individuals over whom suspicion is cast. Moreover, there is some judicial precedent for this notion: courts have recognized, in the past, a family's right to protect their lives from public scrutiny based on the actions of a relative.[218]

The intrusion then violates the relatives' privacy interests in their shared genetic code. And the violation might be that the relative has a right not to have their own genetic information exposed by some distant cousin who does not and likely could not know if the relative would consent to such an exposure. This could be grounded in the fact that, as with cell phone location information, an individual is not knowingly providing access to their genetic information when an unknown distant cousin chooses to waive such privacy. Professor Murphy has likened this shared genetic information to the joint interest held by property owners who share common space:

> As the Court has made clear in *Georgia v. Randolph*, consent by one co-occupant cannot vitiate the constitutional interest asserted by the other co-occupant . . . indeed, to the extent that one occupant could provide consent in the absence of the nonconsenting co-occupant, it was because the co-occupant assumed the risk of such an eventuality upon agreeing to share the space . . . by way of additional comparison, the Court rejected the claim that one occupant's consent could overcome the other's non-consent. Thus, the constitutional authority to search for matches (i.e., the diminished privacy of the offender) is wholly absent with regard to the relative (who retains full privacy entitlements).[219]

---

[217] 23andMe, *The Method Behind the Relative Finder Tool*, 23ANDME (Apr. 19, 2012), https://blog.23andme.com/news/announcements/how-many-relatives-do-you-have/.

[218] Nat'l Archives & Records Admin. v. Favish, 541 U.S. 157, 168–170 (2004) (recognizing a privacy right in protecting from disclosure the details of a relative's death).

[219] Murphy, *Relative Doubt*, *supra* note 53, at 336–37 ("[A] further analogy might be

In essence, other relatives who share genetic information but never gave their consent for it to be exposed should not have their privacy rights ignored.

Unlike the databased person who consented to diminish their privacy rights, the relative never assumed that same risk. However, by consenting to law enforcement's access to their genetic profile, the submitting individual has implicated the privacy rights of innumerable others who share a genetic link. As technology progresses and more matches from further distant relatives are made, the number of individuals who could be subjected to suspicion will grow; indeed, if investigators go back far enough, they can find a killer inside all of us.

Whether there are any constitutional limitations on the government's ability either to search for a partial match or to obtain the identity of relatives of the match once a partial match is found is uncertain. Certainly, however, "Fourth Amendment analysis seems appropriate where law enforcement requests the identity of a pivot after a partial or familial match has been found."[220]

Forensic exploitation of commercial genetic databases by law enforcement is relatively new, and the technology changes rapidly, so many of the questions facing the courts with regard to this technology have not been addressed. But the extent of this technology should not be understated. And the highly personal nature of the information should be a factor in being more protective of privacy since the information at stake is not extrinsically observable like the location information at issue in *Carpenter* was. This distinction has significance because the Government argued in *Carpenter* that it could have observed the location information related to the defendant without a warrant; that argument cannot be made with respect to genetic information.[221] Judges could be similarly concerned with the growth and invasiveness of this technology as they were with cell phones in *Carpenter* and *Riley* or the GPS tracking in *Jones*. If they are, they

drawn to *Steagald v. United States*, 451 U.S. 204, 219 (1981), in which the Court noted that the Constitution may require a search warrant to execute an arrest warrant for an individual in the home of a third party. Just as the law-abiding individual does not forfeit personal privacy merely by associating with the potential arrestee, so too should the law-abiding relative not be deemed to forfeit personal privacy by mere accident of biological relation.").

[220] Jessica D. Gabel, *Probable Cause from Probable Bonds: A Genetic Tattle Tale Based on Familial DNA*, 21 HASTINGS WOMEN'S L.J. 3, 37 (2010).

[221] *See* 138 S. Ct. 2206, 2217 (2018).

might find that there is a search in one of these steps and that at a minimum a warrant is required for access to this kind of information.

V. PHILOSOPHICAL CONSIDERATIONS

Radical shifts in the nature and intrusiveness of technology, as well as evolving conceptions of privacy, have rendered traditional modes of thinking about both outdated. Judges have remarked on this as recently as *Carpenter* and *Riley*, but also before that in *Jones* and some of the other cases mentioned above. However, such issues have only been addressed in a piecemeal manner, invalidating searches where the reach of certain technologies has exceeded the courts' comfort level, leaving the larger privacy doctrine intact but cracking. In particular, high-tech surveillance and investigative techniques, like law enforcement's use of DTC databases, represent a surging expansion of technology likely not contemplated by those justices who crafted the third-party doctrine, to say nothing of the founders who created the legal regime providing our privacy protections. In fact, few people even knew that DTC databases were being used to solve crimes until the GSK was identified. More than piecemeal jurisprudence is required to tackle the complex legal issues at stake. An updated political and philosophical foundation for privacy needs to be poured.

In the eighteenth century, British philosopher Jeremy Bentham conceived of a novel type of prison called a "panopticon."[222] It was a place where inmates could be constantly surveilled without knowing they were being surveilled, as the watchman would be hidden from their view.[223] Central to the concept was the fact that while only one watchman was actually watching and thus could not watch everyone at once, because the prisoners did not know when they were being watched, they were effectively compelled to regulate their own behavior as if they were being watched at all times.[224] Bentham's Panopticon has been noted as a metaphor for the "mechanisms of large-scale social control that characterize the modern world."[225]

It is not difficult to see how a far more potent version of Bentham's panopticon applies to expansive technology today.[226]

---

[222] Jeremy Bentham, *Panopticon, or, the Inspection-House, in* THE WORKS OF JEREMY BENTHAM 40–41 (John Bowring ed., 1964).

[223] *Id.*

[224] *Id.*

[225] MICHAEL FOUCALT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 200 (1979).

[226] The current reality is far more powerful because many are watching and, even if they

CCTV provides near constant surveillance over our movements even if most of the time no one will ever view this footage. Facebook and Google track preferences based on our internet searches. The recently disclosed NSA bulk-collection programs, which collected, among many other forms of data, calls made, texts sent, and contents of email address books, demonstrate the extent to which the technologically charged panopticon has arrived and the extent to which we have no control over whether we are being watched or not. Many of the technologies we think of as intertwined with life in the 21st century come with the price of increased surveillance. As the Golden State Killer case shows, genetic databases are in fact just another example. By opting into a genetic database, one further expands the reach of the technological panopticon—granting law enforcement viewing access to critical genetic information that could identify individuals or traits about them, as well as the identities of scores of their relatives who never opted into the databases and may have affirmatively chosen not to do so.

Alongside increased surveillance, expectations of privacy have shrunk. Americans now seem to simply assume that their use of various technologies requires surrendering to a higher degree of surveillance.[227] Those who continue to value their privacy have to take affirmative actions to do so. They may "put Post-it notes over their computer cameras, watch what they tweet or post on Facebook, or write their emails as if some omnipresent eye is reading over their shoulders."[228] While this once might have seemed like paranoid behavior, it now seems reasonable if not even advisable as a method of self-defense and preemptive protection. What the cumulative effects of such a resignation to near-constant surveillance will be is unknown, but they seem harmful to the health of a free, vibrant society.

One might think that giving up the ability to trace one's

are not, so much is recorded that can be watched later even if not in real time.

[227] *See, e.g.*, Fact Tank, *Most Americans Think the Government Could Be Monitoring Their Phone Calls and Emails,* PEW RESEARCH CENTER (Sept. 27, 2017), https://www.pewresearch.org/fact-tank/2017/09/27/most-americans-think-the-government-could-be-monitoring-their-phone-calls-and-emails/ ("Seven-in-ten U.S. adults say it is at least somewhat likely that their own phone calls and emails are being monitored by the government.").

[228] Matthew Harwood & Christopher Calabrese, *Tomgram: Calabrese and Harwood, Privacy Down the Drain*, TOMDISPATCH (Sept. 22, 2013, 4:29 PM), http://www.tomdispatch.com/blog/175750/tomgram%3A_calabrese_and_harwood,_privacy_down_the_drain/.

ancestry on a genealogy site does not rise to the same level of inconvenience as would not participating in many other technologies, such as driving or use of cell phones and email, or that the particular surveillance in the case of commercial genetic databases is not as severe. But this is the wrong way to think about the privacy issues at stake. It is obvious what the benefits of these genetics databases are, and they are significant with respect to identity, family, personal history, and health, among other things. If, however, in order to use these databases one is required to dive deeper into the technology panopticon, some will be deterred from enjoying the benefits of those sites. Others will just resign themselves to being subjects of another form of surveillance, a layer of their privacy stripped away. And still others who are identified by the genetic databases but have not themselves opted in (such as the 73-year-old misidentified man in the GSK case) suffer privacy harms that are, in fact, not of their own doing and thus, for them, unable to be defended against. For them, there is no way to escape the dragnet. Such individuals' right to be left alone is violated, and in its place is a world in which the details of our lives become data or evidence exposed to the government's clinical gaze.[229]

There is a kind of cruel exploitation at work here. It is a very human, even visceral, desire to want to trace one's lineage, to reconnect with lost or undiscovered relatives, to see where one is located in the human chain and to generally want to know more about oneself. But that desire is exploited in a number of different ways. First, individuals who have an interest in shaping and editing their own lives are surrendering a depiction of their life to a third party who shapes it for them.[230] When law enforcement gains access to one's genetic profile, it obtains significant biographical information beyond that which the individual herself might have. The privacy interest includes a loss of control over a person's DNA, which, at least biologically, is their very self. Second, those who actively avoided databases are now brought into the government's view and identifiable

[229] Jeffrey H. Reiman, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, 11 SANTA CLARA HIGH TECH. L.J. 27, 28 (1995) (explaining that the term "clinical gaze" refers to a method by which the government exerts social control over a population by increasing its ability to observe people even if they do not know they are being observed); *see also* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy,* 4 HARV. L. REV. 193 (1890).

[230] Reiman, *supra* note 229, at 40 ("Intelligent Vehicle Highway Systems contain information on where travelers go, the routes they use, and when they travel.").

because of another's decision. The latter exploitation was apparent in the Golden State Killer case where law enforcement investigated some particularly vulnerable individuals who had not been users of DNA databases.

The privacy intrusion involved in law enforcement's use of genetic databases might be justified on utilitarian grounds in some instances. "The ends justify the means" response is enough for some to set aside the principles underlying the Fourth Amendment.[231] Indeed this argument gains force as brutal and high-profile killers, such as the Golden State Killer, are caught using this technology. But this comes at a cost. The cost is the privacy intrusion individuals necessarily incur, and the risk is the potential for the increasing use of this technology in the context of lesser crimes and even non-criminal matters: "if these techniques became widely used there's a risk a lot of innocent people would be caught in a web of genetic suspicion and subject to heightened scrutiny," says Jennifer Mnookin, Dean of UCLA Law and founder of UCLA's program on understanding forensic science evidence.[232] Mnookin further notes that she sees the use of genetic databases as a step toward a genetic surveillance state. "That's what's hard about this," she says "we don't have a blood taint in this country . . . guilt shouldn't travel by familial association, whether your brother is a felon or an amateur genealogist . . . it is beginning to dawn on consumers that even their most intimate digital data—their genetic profiles—may be passed around in ways they never intended."[233]

It is a likely proposition that not every investigator employing DTC databases will be hunting the Golden State Killer. Instead, investigators may use these databases when they would be helpful, regardless of the wrongness of the criminal conduct. In May 2018, the remains of a 19-week-old fetus were found in a Georgia sewer—almost certainly the result of a miscarriage.[234] Had the fetus been 20 weeks old and the result of an abortion, the fetal death would have been

[231] Judy G. Russell, *The Price of Sharing*, THE LEGAL GENEAOLOGIST (May 27, 2018), https://www.legalgenealogist.com/2018/05/27/the-price-of-sharing/.

[232] Molteni, *Creepy Genetics*, *supra* note 66.

[233] *Id.*

[234] Russell Brandom, *Police Are Using DNA Testing to Track Down a Fetus's Mother*, THE VERGE (May 10, 2018, 3:03 PM), https://www.theverge.com/2018/5/10/17340666/dna-testing-georgia-fetus-codis-abortion-genetics-investigation.

a criminal offense.[235] The Georgia Bureau of Investigation conducted DNA testing to identify the mother, claiming that the mother needed to be identified to make sure she was healthy and safe or to allow her to inter the fetus.[236] This was unlikely to be the full explanation given that it takes up to a year to test remains and no one recommended identifying the father to allow him to inter the fetus.[237] "Clearly, this is being treated as a crime — a wrong worthy of investigation."[238] Now, genealogy companies are affirmatively availing themselves to law enforcement's use for much less serious crimes, such as robbery, so many of the early fears of genealogists have already come to fruition.

In most instances in which DTC databases have been searched to solve cold cases, the ends might be argued to justify the means, i.e., the privacy intrusions are justifiable in order to catch a serial murderer or rapist. This is at least arguably the case in the Golden State Killer investigation. Clearly, however, there are cases in which some people might think that the ends do not justify the means, and would not welcome the use of their DNA results, as in the case of the mother in the Georgia case or in the case of Uighur internment in China. Or imagine the information were used for civil purposes such as denying or pricing insurance, or to allow adoption or not. Here lies a potential conflict. If we are satisfied with an ends-justify-the-means impetus for the use of DTC databases, we would need a principled way of distinguishing which ends justify which means. This is a difficult task that we have not yet accomplished. It would require a political and philosophical view translated into legislative consensus or possibly new judicial doctrine. Instead, the status quo is that the government has relatively unregulated access to these databases and may be able to access them whenever "something is defined by government somewhere at some time as a wrong worthy of investigation."[239] We may not always—or someday, even often—agree with the government's definition.

Nor does everyone even accept the justification that the ends

---

[235] *Id.*

[236] *Id.*

[237] Nefeteria Brewster, *Fetus Identification Could Take up to a Year, Says Coroner*, AUGUSTA CHRONICLE (May 9, 2018, 2:32 PM), https://www.augustachronicle.com/news/20180509/fetus-identification-could-take-up-to-year-says-coroner.

[238] Russell, *supra* note 231.

[239] *Id.*

justify the means. Public reaction to law enforcement's exploitation of such services has been mixed.[240] Some note that they would be fine with law enforcement's use of genetic information: "I'll volunteer to give my DNA and out any of my cousins who may be rapist/murderers. So much drama over nothing," wrote Stu Pike, who used GEDmatch to track down his relatives.[241] Others not so much: "My relatives consented for their data to be used for genealogy but not for criminal investigations."[242] "I've had many sleepless nights the last few years, realizing that it's coming," CeCe Moore, a genealogist noted of her profile possibly being used in a law enforcement investigation.[243]

Clearly a forthcoming question with which we must grapple is whether such privacy intrusions can be justified in the name of solving cold cases, if so with what protections? And, if not, how can we create a legal regime of genetic searching that effectively balances crime-solving and privacy?

CONCLUSION

This article initially set out to determine whether the forensic use of DTC databases should be considered a Fourth Amendment search subject to a warrant requirement. In the process of doing so, it has identified the harms inflicted by the forensic deployment of DTC databases and has performed the kind of comprehensive balancing analysis that a court should perform. The Golden State Killer case provides insight into some of these harms as well as the benefits DTC databases provide law enforcement; it has also raised new Fourth

---

[240] Christi J. Guerrini et al., *Should Police Have Access to Genetic Genealogy Databases? Capturing the Golden State Killer and Other Criminals Using a Controversial New Forensic Technique*, 16 PLOS BIOLOGY (Oct. 2, 2018) ("[A]mong the 1,587 respondents the majority supported police searches of genetic websites that identify genetic relatives (79%) and disclosure of DTC genetic testing customer information to police (62%), as well as the creation of fake profiles of individuals by police on genealogy websites (65%). However, respondents were significantly more supportive of these activities (all $p < 0.05$) when the purpose is to identify perpetrators of violent crimes (80%), perpetrators of crimes against children (78%), or missing persons (77%) than when the purpose is to identify perpetrators of nonviolent crimes (39%). Notably, a similar line was drawn by GEDmatch in its updated privacy policy, adopted after the survey was closed, which explicitly permits law enforcement to search GEDmatch for matches to DNA left at scenes of violent crimes, defined by the site as homicide and sexual assault.").

[241] Kolata & Murphy, *supra* note 85.

[242] *Id.*

[243] *Id.*

Amendment questions. Meanwhile, *Carpenter* has, to a degree, shifted the Fourth Amendment landscape. This dynamic has compelling implications for the case of DTC databases. From this analysis, it has become clear that Fourth Amendment jurisprudence can no longer be mechanically applied such that certain technologies are categorically searches or not, as traditional third-party doctrine has divided the world of privacy. Such a binary system is contrived and does not reflect how people and technology interact in the modern world. Instead, courts should enter the fray as arbiters of the individual characteristics of a particular technology. In the case of DTC databases, courts should adopt the balancing test proposed here as a model for understanding the harms involved and the different actors upon whom a search could be performed. They must examine: the utility of the technology to law enforcement, the harms it causes to different actors, and the different points in the investigative process in which the intrusions are greatest.

The harms both current and future caused by the forensic exploitation of commercial genetics are not inevitable, and need not be unconstrained. First, one could more strictly circumscribe the number of times or circumstances under which a familial search can be performed. Law enforcement could prioritize based on which searches are likely to provide the most significant social benefit. In other words, such searches might only be used for serious crimes such as murder and rape, and as more classically federal examples, terrorism, espionage, and other national security issues.

Second, for the government to undertake a genetic search, law enforcement might be required to demonstrate to a judge that it had exhausted all other less intrusive investigatory tactics, and that no viable suspects were identified. This way law enforcement is not tempted to use genetic database searches as a shortcut rather than a near-final investigatory step. Moreover, as indicated above, the subsequent investigation that takes place after matches are identified in which law enforcement pursues relatives of the matches could also be more strictly regulated and possibly require subsequent reports to the judge.

Third, some of these controls and representations could be embodied in a warrant requirement. A warrant would provide a degree of judicial oversight in the investigative process that is currently lacking. Not only would a warrant provide protection by setting forth the basis for a probable cause finding by a judge, it could document the other burdens the government might be required to satisfy. For

example, the warrant could also require the government to make specific and limiting commitments about how it will conduct the search and maintain the genetic information obtained—commitments which could ensure additional protection for databased persons and their relatives. A warrant could also require a showing of the exhaustion of other investigative techniques, as is required in Title III warrants used for wiretaps.[244] Indeed, as is also the practice with Title III wiretaps, there might even be a requirement of subsequent reports to determine if the searching should continue, be expanded or shut down.[245]

On the other hand, the requirement of probable cause in a warrant is somewhat inapposite in the genetic context. This is because the warrant would not actually be putting forth probable cause of finding evidence of a crime, but rather putting forth probable cause that, at best, the search of the DTC database would yield someone who provides a genetic link to the perpetrator of the crime. The chance that the perpetrator would actually be on the particular database is extremely low and certainly far below what would be required for probable cause normally. If the standard were instead to apply to the overall likelihood of finding a familial match to the crime scene DNA source, certainly the standard would be met as there is a very high likelihood that officers will find a relative of almost anyone. But this would be a very different inquiry than normal probable cause, as it would not be a search for the perpetrator of a crime, but rather for a person who might potentially lead investigators to the perpetrator. In this sense, it is more like a warrant for a material genetic witness—someone who may be able to provide evidence that is a link of indeterminate remove to a crime but is not considered a perpetrator.[246] All of this is a convoluted and novel basis for a warrant that does not fit neatly within the orthodox doctrine of probable cause and warrants.[247]

Moreover, as demonstrated by the efforts in California, law enforcement has made a concerted effort to shutter their exploitation of DTC databases from the public eye, so the privacy intrusions

---

[244] *See* 18 USC § 2518(1); 18 USC § 2518(4).

[245] *See* 18 USC § 2518(2).

[246] *See* 18 USC § 3144 (material witness rule).

[247] *See* Orlando Police Department Search Warrant, *supra* note 77 (as noted above, a warrant has been issued for access to GEDmatch on at least one occasion, but the probable cause section has not been made available to the public).

discussed in this article are insulated from public backlash to some extent, as are the specific probable cause justifications required for a warrant.[248] When the actual operation of law enforcement is sequestered, when it is out of sight, we are not forced to morally reflect on it, and it is out of mind. Thus, the time is now to examine these practices before they proliferate—fostered by a legal framework that represses transparency.

Courts should keep all of this in mind when they are performing a balancing test, noting the harms, the possible points of search, and the benefits and drawbacks of limiting the ability of law enforcement to use DTC databases, assuming that the legislatures do not choose to step in and try to define what can and cannot be done in this area.

The advent of direct-to-consumer genetic databases provides law enforcement near-boundless opportunity to solve crimes that were previously unsolvable, and find individuals previously unfindable. This powerful and important ability, however, is not without consequence. The collateral harms inflicted alongside law enforcement's access to genetic technology must be acknowledged, and decisions made about its permissibility should seek to minimize those harms where possible. Such an approach will protect liberty in the face of inevitable and creeping surveillance technology.

[248] St. John, *supra* note 60 (quoting Professor Erin Murphy: "[t]hey're afraid that if the public finds out what we're doing, we won't be allowed to do it anymore. So the solution is, '[d]on't tell the public . . . .'").