St. John's Law Review

Volume 93
Number 3 *Volume 93, 2019, Number 3*

Article 10

DNA Is Different: An Exploration of the Current Inadequacies of Genetic Privacy Protection in Recreational DNA Databases

Jamie M. Zeevi

NOTES

DNA IS DIFFERENT: AN EXPLORATION OF THE CURRENT INADEQUACIES OF GENETIC PRIVACY PROTECTION IN RECREATIONAL DNA DATABASES

JAMIE M. ZEEVI[†]

"You may never commit a crime. But how should you feel if your DNA was used to locate a distant relative who did?"[1]

INTRODUCTION

Joseph James DeAngelo Jr., more infamously known as the Golden State Killer,[2] committed at least one hundred burglaries, raped at least fifty women, and murdered at least twelve people between 1974 and 1986.[3] It took law enforcement officials more than forty years to identify him.[4] Ray Charles Waller, recently identified as the NorCal Rapist, attacked and raped at least eleven

[†] Managing Editor, *St. John's Law Review*; J.D. Candidate, 2020, St. John's University School of Law; B.A., 2012, Washington University in St. Louis. With many thanks to my family for their unwavering love, support, and encouragement, and to the members and editors of the *St. John's Law Review* for their hard work and assistance in preparing my Note for publication.

[1] 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.

[2] While most widely known as the Golden State Killer, DeAngelo has also been "variously called the East Area Rapist, Original Nightstalker, Diamond Knot Killer and Visalia Ransacker . . . ." Justin Jouvenal, *To Find Alleged Golden State Killer, Investigators First Found His Great-Great-Great-Grandparents*, WASH. POST (Apr. 30, 2018), 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.

[3] *Id.*; *see also* Benjy Egel, *Here's the String of Crimes Tied to the East Area Rapist in Years of California Terror*, SACRAMENTO BEE (Apr. 29, 2018, 4:52 AM), https://www.sacbee.com/news/local/crime/article209788654.html.

[4] Jouvenal, *supra* note 2.

women between 1991 and 2006.[5] It took law enforcement officials more than twenty-seven years to identify him.[6] William Earl Talbott II was arrested in May 2018 for a double murder committed thirty years earlier, in 1987.[7]

In each of these cases, investigators identified the suspects using a technique called "familial DNA searching,"[8] by which investigators match DNA found at crime scenes to the DNA of family members in DNA databases.[9] While conducting familial DNA searches in criminal DNA databases like the Combined DNA Index System ("CODIS") is still a relatively new technique,[10] conducting such searches in recreational DNA databases is brand new.[11] And this is only the beginning. For example, as of May

---

[5] *See* Sam Stanton, Benjy Egel, Darrell Smith & Cynthia Hubert, *NorCal Rapist Suspect Arrested. He's a 58-Year-Old Safety Specialist at UC Berkeley*, SACRAMENTO BEE (Sept. 23, 2018, 3:00 AM), https://www.sacbee.com/news/local/crime/article218793610.html.

[6] *See id.*

[7] *See* Caleb Hutton & Rikki King, *Suspect Arrested in 1987 Deaths of Young Couple From BC*, HERALD NET (Everett, Wa.) (May 18, 2018, 8:55 PM), https://www.heraldnet.com/news/suspect-arrested-in-1987-deaths-of-young-couple-from-bc/.

[8] Tina Hesman Saey, *New Genetic Sleuthing Tools Helped Track Down the Golden State Killer Suspect*, SCI. NEWS (Apr. 29, 2018, 9:49 AM), https://www.sciencenews.org/article/golden-state-killer-suspect-dna-genetics-genealogy ("Investigators . . . used a public genealogy database, GEDmatch, to connect crime scene evidence to distant relatives of Joseph James DeAngelo."); Stanton et al., *supra* note 5 ("The investigation was nearly a carbon copy of the one that led authorities to . . . Joseph James DeAngelo. . . . [I]nvestigators . . . entered DNA from the NorCal Rapist crime scenes into a 'genetic genealogy' website called GEDmatch . . . ."); Hutton & King, *supra* note 7 ("[William Earl Talbott] was determined to be the only potential suspect through . . . the same technique used to find the suspected Golden State Killer . . . .").

[9] *See* Frederick R. Bieber, Charles H. Brenner & David Lazer, *Finding Criminals Through DNA of Their Relatives*, 312 SCI. 1315, 1315 (2006).

[10] United States' national forensic DNA database, CODIS, was formally established in 1994. *Combined DNA Index System (CODIS)*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis (last visited Aug. 29, 2019). Familial searching in forensic DNA databases was first used in the United Kingdom in 2001 to identify Joseph Kappen as the Saturday Night Strangler. *Science of the Future: Identifying Criminals Through Their Family Members*, DNA FORENSICS, http://www.dnaforensics.com/familialsearches.aspx#kappen (last visited Aug. 29, 2019); *see also* Kevin Toolis, *The Hunt for the Saturday Night Strangler*, THE GUARDIAN (London) (Jan. 17, 2003, 7:48 PM), https://www.theguardian.com/lifeandstyle/2003/jan/18/weekend.kevintoolis. The first United States case solved using this method to search in CODIS was solved in 2009. *See* Jim Spellman, *Using Relative's DNA Cracks Crime, but Privacy Questions Raised*, CNN (Nov. 18, 2009, 3:56 PM), http://www.cnn.com/2009/CRIME/11/17/colorado.family.dna/index.html.

[11] *See* The Golden State Killer case was the first successful use of familial searching in a recreational DNA database. Dan Vergano & Virginia Hughes, *A Serial*

2018, Parabon NanoLabs, a forensic DNA analysis company, had already uploaded about one hundred crime scene DNA samples to GEDmatch and found third cousin or closer matches for twenty of these samples.[12] As the use of familial DNA searching in recreational DNA databases becomes a more prevalent tool in forensic investigations, consideration must be given to individuals' genetic privacy, and statutory protections must be implemented regarding law enforcement's access to, and use of, this information.

Throughout the United States, hobbyists and curious individuals are voluntarily "buil[ding a] . . . genetic panopticon" in recreational DNA databases, using services like AncestryDNA, 23andMe, MyHeritage DNA, and FamilyTreeDNA, among others, to do so.[13] Furthermore, public recreational websites like GEDmatch provide people the opportunity to upload their raw DNA data for free in order to cross-reference their results with the results of individuals who have used similar services from other companies.[14] While exploring genealogy to discover where one's ancestors came from, to build one's family tree, or to connect with

---

Killer Was Caught Because Investigators Found His Family's DNA on a Website, BUZZFEED NEWS (Apr. 27, 2018, 10:33 AM), https://www.buzzfeednews.com/article/danvergano/serial-killer-dna-testing.

[12] Sarah Zhang, *The Coming Wave of Murders Solved by Genealogy*, THE ATLANTIC (May 19, 2018), https://www.theatlantic.com/science/archive/2018/05/the-coming-wave-of-murders-solved-by-genealogy/560750/ [hereinafter Zhang, *The Coming Wave of Murders Solved*]. These numbers continue to grow. Parabon NanoLabs stated that as of December 2018, it had uploaded over two hundred DNA profiles to GEDmatch. Megan Molteni, *The Future of Crime-Fighting is Family Tree Forensics*, WIRED (Dec. 26, 2018, 8:00 AM), https://www.wired.com/story/the-future-of-crime-fighting-is-family-tree-forensics/. In 2018, genetic genealogy was used as a tool in two hundred cases. As of December 2019, genealogy searches in GEDmatch helped "law enforcement [to] solv[e] over 70 cold cases in the U.S." Kameran Wong, *A Message to Verogen Customers about the GEDmatch Partnership*, VEROGEN (Dec. 10, 2019), https://verogen.com/a-message-to-verogen-customers-about-the-gedmatch-partnership/ (last visited Jan. 20, 2020).

[13] Matt Ford, *How the Supreme Court Could Rewrite the Rules for DNA Searches*, NEW REPUBLIC (Apr. 30, 2018), https://newrepublic.com/article/148170/supreme-court-rewrite-rules-dna-searches; *see also* Antonio Regalado, *2017 Was the Year Consumer DNA Testing Blew Up*, MIT TECH. REV. (Feb. 12, 2018), https://www.technologyreview.com/s/610233/2017-was-the-year-consumer-dna-testing-blew-up/.

[14] *See* Susan Scutti, *What the Golden State Killer Case Means for Your Genetic Privacy*, CNN (May 1, 2018, 12:01 AM), https://www.cnn.com/2018/04/27/health/golden-state-killer-genetic-privacy/index.html [hereinafter Scutti, *What the Golden State Killer Case Means*].

one's distant or long-lost relatives may be exciting, unrestricted access to this DNA data may result in unwarranted invasions of people's privacy.

It is possible to discern from one person's DNA the identities of others to whom that person is biologically related.[15] Each individual in a DNA database is like "a beacon that illuminates hundreds of distant relatives . . . . [I]t's enough to have your third cousin or your second cousin once-removed in these databases to actually identify you."[16] In fact, a recent study suggests that the DNA in these databases will soon have the potential to identify nearly everyone.[17] Beginning with a DNA database containing samples from 1.3 million individuals, investigators were able to narrow a person's identity to fewer than twenty individuals simply by inputting "basic information such as someone's rough age."[18] Notably, this study found that this search method has the potential to identify sixty percent of Americans with European heritage regardless of whether many of those people had ever submitted their genetic information to a recreational DNA database.[19] For perspective, 23andMe boasts more than five

---

[15] *See* Kelly Lowenberg, *Applying the Fourth Amendment When DNA Collected for One Purpose is Tested for Another*, 79 U. CIN. L. REV. 1289, 1294 (2011) ("A partial match between two DNA samples indicates that the two donors have a common genetic lineage."). "A sibling shares half of [one's] genetic profile. A cousin shares an eighth." Carolyn Johnson, *Even If You've Never Taken a DNA Test, A Distant Relative's Could Reveal Your Identity*, WASH. POST (Oct. 11, 2018, 2:00 PM), https://www.washingtonpost.com/science/2018/10/11/even-if-youve-never-taken-dna-test-distant-relatives-could-reveal-your-identity/. Furthermore, information gleaned from one person's DNA can disclose information about the rest of that person's family. *See* Kolata & Murphy, *supra* note 1.

[16] Rob Stein, *Easy DNA Identifications With Genealogy Databases Raise Privacy Concerns*, NPR (Oct. 11, 2018, 3:58 PM), (quoting Yaniv Erlich), https://www.npr.org/sections/health-shots/2018/10/11/656268742/easy-dna-identifications-with-genealogy-databases-raise-privacy-concerns. Yaniv Erlich is an expert in the field of computational human genetics, as well as a New York Genome Center Core Member and an Associate Professor of Computer Science and Computational Biology at Columbia University. COLUMBIA UNIV. DATA SCI. INST., https://datascience.columbia.edu/yaniv-erlich (last visited Sep. 15, 2019). He is also the Chief Science Officer at MyHeritage. *MyHeritage Management Team*, MYHERITAGE, https://www.myheritage.com/management/yaniv_erlich (last visited Sep. 15, 2019).

[17] Jocelyn Kaiser, *We Will Find You: DNA Search Used to Nab Golden State Killer Can Home in on About 60% of White Americans*, SCI. MAG. (Oct. 11, 2018, 2:00 PM), https://www.sciencemag.org/news/2018/10/we-will-find-you-dna-search-used-nab-golden-state-killer-can-home-about-60-white ("In a few years, it's really going be everyone." (quoting Yaniv Erlich)).

[18] *Id.*

[19] Malcolm Ritter, *Study: DNA Websites Cast Broad Net for Identifying People*, MED. XPRESS (Oct. 11, 2018), https://medicalxpress.com/news/2018-10-dna-websites-broad-net-people.html. This study was conducted using DNA samples of individuals

million customers, while AncestryDNA boasts ten million,[20] and GEDmatch has stated that it sees almost one thousand new uploads per day.[21] And these are just a few of all the recreational DNA services currently available.

Furthermore, government, law enforcement, and the general public currently have wide access to the DNA collected and stored in public recreational DNA databases like GEDmatch. In fact, until the news broke explaining the method investigators used to identify the Golden State Killer, even the operators of GEDmatch were unaware that police could use such websites for criminal investigations, illustrating how little people consider the ramifications of submitting their raw DNA data to such websites.[22] As recreational genealogy services become increasingly popular, law enforcement will likely become more enthusiastic about the investigation potential that familial searching in these databases holds. While familial searching may be an effective way to catch violent criminals, the use of familial DNA in forensic investigations is a new legal frontier, and regulations of whose DNA data may be accessed or used, by whom, when, and how, are spotty and unclear.[23] In fact, there are currently no legal restrictions on familial searching in recreational DNA databases.[24]

---

with European descent, as this was the largest group in the database used. *Id.* GEDmatch's database currently "only encompasses about 0.5% of the U.S. adult population. . . . Once the GEDmatch figure rises to 2%, more than 90% of people of European descent will have a third cousin or closer relative and could be found in this way." Kaiser, *supra* note 17. FamilyTreeDNA, a site similar to GEDmatch, also allows law enforcement to use its databases to conduct familial searching, which "roughly doubles the number of genetic profiles cops may use." Kristen V. Brown, *No One is Safeguarding Your DNA*, BLOOMBERG (Feb. 26, 2019, 5:18 PM), https://www.bloombergquint.com/businessweek/law-enforcement-can-do-whatever-it-likes-with-consumer-dna-data.

[20] Kolata & Murphy, *supra* note 1.

[21] Molteni, *supra* note 12.

[22] *See* Justin Jouvenal, Mark Berman, Drew Harwell & Tom Jackman, *A Genealogy Site Led Police to the Golden State Killer. Who Else Can Tap Into This DNA 'Treasure Trove'?*, CHI. TRIB. (Apr. 28, 2018, 4:47 PM), http://www.chicagotribune.com/news/nationworld/ct-golden-state-killer-dna-implications-20180428-story.html.

[23] For example, some states allow familial searching in forensic DNA databases, and some do not. 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-database/561695/ [hereinafter Zhang, *How A Tiny Website*].

[24] *See* Scutti, *What the Golden State Killer Case Means*, *supra* note 14 ("[L]egally, it's the Wild West when it comes to commercial genetic testing companies.").

The lack of legal restrictions and regulations on the use of recreational DNA databases is concerning, as there is nothing to prevent the potential abuse of this practice by law enforcement or by civilians.[25] First, the current lack of restrictions allows this technique to be utilized to investigate any crime at any time. While supporters argue that this technique is helpful in solving violent murder and rape cases, there is currently "no downward limit" on when or on which types of crimes law enforcement may use familial DNA searching in recreational databases.[26] Familial DNA searching was recently used for the first time as a tool in an assault investigation.[27] Once police identified the suspect, a seventeen-year-old high school student, police directed the school resource officer to surveil the student in the cafeteria and to collect the student's discarded milk and juice cartons for use in confirming the DNA match.[28] The school resource officer did so.[29] It is not a far leap from using familial DNA searching in murder and rape investigations to using it in assault investigations. It is also not difficult to imagine the next leap—the use of the technique in petty crime investigations.

---

[25] *See* Stein, *supra* note 16 ("The police currently [are] using these techniques to find . . . [murderers] and bad people, . . . But are we OK with using this technique to identify people in a political demonstration who left their DNA behind?"); *see also* Nila Bala, *We're Entering a New Phase in Law Enforcement's Use of Consumer Genetic Data*, SLATE (Dec. 19, 2019, 7:30 AM), https://www.slate.com/technology/2019/12/gedmatch-verogen-genetic-genealogy-law-enforcement.html (noting unsettling possibilities "including having our genes held ransom," and "people pretending to be our relatives asking for our help"); 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 ("In Texas, police met search guidelines by classifying a case as sexual assault but after an arrest only filed charges of burglary. [In California], prosecutors have persuaded a judge to treat unsuspecting genetic contributors as "confidential informants" and seal searches so consumers are not scared away from adding their own DNA to the forensic stockpile."). While beyond the scope of this Note, because the DNA in recreational databases is not legally protected, it is also foreseeable that familial searching in websites like GEDmatch may be used by drug and insurance companies to do things like targeting advertising or building out "vast networks of relatedness to determine [insurance] risk." Brown, *supra* note 19.

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

[27] *Id.*

[28] *Id.*

[29] *See id.*

Second, there is currently no legal recourse for someone whose DNA, or whose genetic relatives' DNA, was utilized in a criminal investigation.[30] No clear remedies exist for "mistakes, the discovery of embarrassing or intrusive information, or misuse of the information."[31] Furthermore, law enforcement increasingly outsources its familial DNA searching to forensic companies and individual genetic genealogists.[32] However, genetic genealogy is a profession that currently has neither formal rules nor "academic training or certification program[s]," to ensure the quality of work provided.[33] Law enforcement's unrestricted use of familial DNA searching in recreational databases and its outsourcing of this work, combined with the tremendously revealing nature of DNA, creates the perfect storm for errors, abuse, or both.

Additionally, relatives of individuals who voluntarily submit their DNA samples to recreational genealogy websites do not have adequate means available to protect their own genetic privacy. Current constitutional and statutory protections do not protect voluntarily submitted DNA stored in recreational DNA databases. Moreover, traditional understandings of the legal considerations around privacy do not map onto DNA data. DNA is different. Given our lack of knowledge regarding the potential of DNA as well as the lack of regulations regarding the use of this DNA data, it is imperative that statutory protections are implemented.

Part I of this Note discusses the fundamental science behind DNA and defines and explains the process of familial DNA searching. Part I also discusses how *Carpenter v. United States* provides a framework to begin thinking about the unique nature of DNA and privacy implications for its use, and why the revealing nature of this type of data warrants protection. Part II of this Note delves into the lack of constitutional and statutory protections for DNA in recreational DNA databases. First, Part II explains that traditional Fourth Amendment concepts, like search warrants, probable cause, reasonable expectation of privacy, third-party doctrine, and consent, do not adequately protect or map onto DNA stored in recreational databases. Next, Part II highlights the complete absence of statutory protections for the forensic use of

---

[30] Molteni, *supra* note 12.

[31] Joh, *supra* note 26.

[32] *See* Laura Hautala, *How Sharing Your DNA Solves Horrible Crimes . . . and Stirs A Privacy Debate*, CNET (July 2, 2019, 5:00 AM), https://www.cnet.com/news/how-sharing-your-dna-solves-horrible-crimes-and-stirs-a-privacy-debate.

[33] *Id.*

DNA in this particular context. Part III assesses the strength of common arguments intended to minimize the necessity of statutory protection and concludes that they are not persuasive. Such arguments include the strong government interest in being able to use familial searching to solve and prevent crimes, the anonymization of DNA samples to resolve privacy concerns, and the work-intensive nature of familial searching in these databases tending to decrease the likelihood that the technique would be used frequently. Finally, Part IV asserts that statutory protection is the appropriate solution and that it is imperative to protect the genetic information of individuals stored in recreational DNA databases against invasive use by government actors. Part IV also provides an overview of possible regulations.

I. BACKGROUND

A. DNA and Familial DNA Searching Defined

DNA, which makes up genes,[34] "is an information-rich material contained in every cell in our bodies," and defines who we are in the most fundamental way.[35] To identify individuals in CODIS using their DNA, the Federal Bureau of Investigation ("FBI") analyzes short tandem repeats, also known as STRs or " 'junk' genes."[36] STRs "can be repeated dozens or hundreds of times" throughout an individual's genome, and the number of repeats varies from individual to individual.[37] These junk genes are valuable to the FBI mainly for their ability to identify individuals, as they do not appear to reveal historical medical or clinical information about a person.[38] "Each [CODIS] profile looks for STRs in up to 20 locations in the human genome."[39] In contrast, recreational DNA databases do not use STRs and instead use single nucleotide polymorphisms ("SNPs"), which look for

---

[34] *What is a Gene?*, NAT'L INST. OF HEALTH, U.S. NAT'L LIBRARY OF MED., GENETICS HOME REFERENCE, https://ghr.nlm.nih.gov/primer/basics/gene (last visited Sep. 15, 2019).

[35] Lowenberg, *supra* note 15, at 1292.

[36] Lowenberg, *supra* note 15, at 1293; Erin Murphy, *Law and Policy Oversight of Familial Searches in Recreational Genealogy Databases*, 292 FORENSIC SCI. INT'L e5, e5 (2018). "The adjective 'junk' may mislead the layperson, for in fact this is the DNA region used with near certainty to identify a person." Maryland v. King, 569 U.S. 435, 442 (2013).

[37] Zhang, *How a Tiny Website*, *supra* note 23.

[38] Murphy, *supra* note 36, at e5.

[39] Zhang, *How a Tiny Website*, *supra* note 23.

information at about 600,000 locations in the genome.[40] SNPs are rich in information,[41] and at the very least can be used to trace a person's heritage, identify distant relatives,[42] predict physical appearance, and forecast future wellness and disease propensities.[43] And the use of SNPs by recreational services makes sense when one remembers that "[p]eople submit their DNA to sites like 23andMe or MyHeritage because they want to know *more* about their genetic make-up than just identity."[44]

Whether STRs or SNPs are analyzed, a familial DNA search is defined as "an intentional or deliberate search of [a DNA] database conducted after a routine search for the purpose of potentially identifying close biological relatives of [an] unknown forensic sample associated with [a] crime scene profile."[45] In order to conduct a familial search in a DNA database, investigators first convert recovered crime scene DNA into raw DNA data.[46] They then submit this raw data into a DNA database with the aim of getting a partial match, which would indicate a genetic relative.[47] If a partial match is made, investigators painstakingly build out the perpetrator's genetic family tree[48] and utilize records to zero in on which family members were of the "right age and in the right place to have committed the crime."[49] Once suspects are identified, investigators will work to obtain DNA samples from the suspects "through . . . court order[s] or by surreptitious means"[50] like

---

[40] *Id.*

[41] Murphy, *supra* note 36, at e5.

[42] Zhang, *How a Tiny Website*, *supra* note 23.

[43] Murphy, *supra* note 36, at e5.

[44] *Id.*

[45] *Frequently Asked Questions on CODIS and NDIS*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet (last visited Oct. 18, 2019).

[46] Nicole L. Cvetnic, *How Police Use DNA 'Familial Searches' to Probe Murders*, SACRAMENTO BEE (Aug. 27, 2018, 5:20 PM), https://www.sacbee.com/news/local/crime/article217427845.html.

[47] *Id.*

[48] *Id.*

[49] Doug Stevens & Maura Dolan, *How Familial DNA Searches Work*, L.A. TIMES (May 9, 2011), http://www.latimes.com/local/lanow/la-me-g-familial-dna-how-it-works-20180426-story.html; *see also* Brown, *supra* note 19 ("The true power of genetic information . . . is realized in conjunction with other online data culled from . . . public records and social networks.").

[50] Cvetnic, *supra* note 46.

surveilling suspects and collecting discarded items that may contain DNA samples.[51] Finally, an individual is confirmed as a suspect if the crime scene DNA matches the collected DNA.[52]

Because CODIS uses STRs, if a familial search in CODIS identifies any partial matches at all, the number will be relatively low. This is because these searches are only capable of identifying "potential sibling[s], parent[s], or child[ren] of the target," whose DNA profiles are already in the CODIS database because they have also come into contact with the criminal justice system.[53] Additionally, basic identification information is nearly the only information available to investigators regarding the individuals affected by these searches.[54] By contrast, because recreational DNA services use SNPs, experts have estimated that the number of partial matches can exceed hundreds, if not thousands, of potential relatives because SNP searches "produce[] leads much farther out—to 'relatives' unlikely to know of each other's relatedness."[55] Significantly, investigators will have access to vast amounts of genetic information regarding the individuals affected by these searches.[56]

For more than forty years, investigators exhausted traditional investigative options trying to identify a suspect for the crimes committed by the Golden State Killer.[57] Although "[c]riminal DNA databases produced no hits," GEDmatch did.[58] In fact, the search in GEDmatch produced between ten and twenty distant cousins.[59] Investigators traced the lineages of these distant cousins to a common ancestor that they shared with the Golden State Killer, which "turned out to be great-great-great grandparents from the early 1800s."[60] They were able to then compile about twenty-five "distinct family trees from the great-great-great grandparents," with the branch that contained Joseph James DeAngelo, Jr. including more than one thousand family members alone.[61]

---

[51] Hautala, *supra* note 32.

[52] Cvetnic, *supra* note 46.

[53] Murphy, *supra* note 36, at e6.

[54] *See id.* at e5 ("Forensic STRs were specifically chosen as "junk" genes—markers with little value other than identification.").

[55] *Id.* at e6.

[56] *See id.*

[57] *See* Jouvenal, *supra* note 2.

[58] *Id.*

[59] *Id.*

[60] *Id.*

[61] *Id.*

The Golden State Killer case is a powerful illustration of the extensive scope of these searches, how many individuals potentially may be included, and why the process of familial DNA searching in recreational DNA databases is so intrusive. The genetic information available to investigators belonging to presumptively innocent individuals in recreational databases is extensive and deeply personal. In fact, "SNPs have not [previously] been used in the criminal justice context" precisely because they are so rich in information.[62] Furthermore, it is currently impossible to fathom all that we will be able to understand in the future from an individual's DNA regarding that individual or her genetic familial network.[63]

For these reasons and more, including the ability to implicate countless individuals with one DNA sample, DNA is different from other types of information, and its use for any purpose—especially in criminal investigations—must be strictly protected. While there may be a strong public interest rationale for conducting familial DNA searches in recreational databases in order to catch violent criminals, there must be limits on how, under what circumstances, and by whom this DNA can be used to avoid potential illegitimate uses. Because DNA is such a unique type of information, how do we begin to think about this type of data and whether and how it should be protected and regulated?

B. Carpenter v. United States *as a Framework for Considering the Uniqueness of DNA Data*

Carpenter v. United States, decided by the United States Supreme Court in June 2018, provides a framework for understanding the type of information contained within DNA and why it requires protection. *Carpenter* concerned an investigation in which the FBI obtained location information for Carpenter for a four-month period in which it suspected Carpenter had committed multiple robberies.[64] "Altogether the Government obtained 12,898 location points [from Carpenter's cell phone

---

[62] Murphy, *supra* note 36, at e5–e6.

[63] For example, forensic experts used DNA "to build three composite images of [a] suspect's likely appearance, an estimate of what he would look like at ages 25, 45, and 65. . . . The faces are educated guesses, based on genetic makeup of DNA found on crime scene evidence." Caleb Hutton, *DNA Analysis Conjures the Possible Face of a 1987 Killer*, HERALD NET (Everett, Wa.) (Apr. 11, 2018, 8:04 PM), https://www.heraldnet.com/news/dna-analysis-conjures-the-possible-face-of-a-1987-killer.

[64] *See* Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

carriers,] cataloging Carpenter's movements—an average of 101 data points per day."[65] Carpenter moved to suppress the cell-site location information ("CSLI"), which the Government planned to use to prove that Carpenter's cell phone was near the sites of the robberies.[66] The case made its way to the Supreme Court, which decided that because of the unique nature of CSLI, the government invaded Carpenter's "reasonable expectation of privacy" in his "physical movements" when it acquired his CSLI information from his wireless carrier.[67]

In determining that CSLI is a unique type of data, the Court described the role of cell phones today as "almost a 'feature of human anatomy' "[68] and as "indispensable to participation in modern society."[69] CSLI is automatically collected when one uses a cell phone "without any affirmative act on the part of the user beyond powering up."[70] The Court continued that because CSLI is collected from everyone who uses a cell phone, and "not just those belonging to persons who might happen to come under investigation[,] this newfound tracking capacity runs against everyone."[71] Describing the nature of CSLI as "deeply revealing,"[72] "detailed, encyclopedic, and effortlessly compiled,"[73] the Court explained that CSLI is capable of "provid[ing] an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, [and] professional . . . associations,' "[74] which "hold for many Americans the privacies of life."[75]

Furthermore, the Court contrasted traditional searches in which police have to establish reasonable suspicion of an individual before tracking their movements, with CSLI, which boasts a uniquely "retrospective quality."[76] The Court noted that with CSLI, "police need not even know in advance whether they

---

[65] *Id.*

[66] *See id.* at 2212, 2213.

[67] *Id.* at 2219.

[68] *Id.* at 2218 (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

[69] *Id.* at 2220.

[70] *Id.*

[71] *Id.* at 2218.

[72] *Id.* at 2223.

[73] *Id.* at 2216.

[74] *Id.* at 2217 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

[75] *Id.* at 2217 (quoting Riley v. California, 573 U.S. 373, 403 (2014)) (internal quotation marks omitted).

[76] *See id.* at 2218.

want to follow a particular individual, or when," because they have the ability to gain access to this information after the fact.[77] Due to the uniquely extensive and revealing nature of CSLI, as well as the availability of CSLI to investigators at any time during an investigation, the Court determined that CSLI is particularly deserving of Fourth Amendment protection.[78]

Read outside the specific factual context of *Carpenter*, the Court's description of this unique type of information, as well as the privacy concerns surrounding it, could just as easily be referring to DNA as to CSLI. While the Court's analysis in *Carpenter* does not map directly onto DNA or address privacy interests in the information of others, DNA data is arguably at least as unique as CSLI, if not more so. Literally a "feature of human anatomy,"[79] DNA, like CSLI, is a profoundly revealing, "detailed, [and] encyclopedic"[80] illustration of who an individual is at the most fundamental level. In contrast to CSLI, DNA is not capable of detailing where a person—or a cell phone—was located at any particular time. However, DNA provides an even more intimate and thorough window into who a person is. DNA is unique in that it has the potential to irrefutably shed light not only on a person's identity, but also on who that person is related to, among many other things. Use of CSLI data does not affect countless people. DNA does. If the *Carpenter* Court considers a person's "familial, political, [and] professional . . . associations"[81] to be "privacies of life,"[82] a person's genetic makeup and genetic family tree surely must be considered at least as private.

Furthermore, while using a cell phone may be "indispensable to participation in modern society,"[83] having DNA is a fact of life. We have DNA by virtue of being human beings, and "[w]e leave [it] everywhere we go. Everywhere we touch has DNA."[84] Moreover, when a distant, unknown relative provides her DNA to a genealogy website, information that implicates countless individuals is collected "without any affirmative act on the

---

[77] *Id.* "[T]he retrospective quality of the data here gives police access to a category of information otherwise unknowable." *Id.*

[78] *Id.* at 2220.

[79] *Id.* at 2218 (quoting *Riley*, 573 U.S. at 385).

[80] *Id.* at 2216.

[81] *Id.* at 2217 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

[82] *Id.* at 2217 (quoting *Riley*, 573 U.S. at 403).

[83] *Id.* at 2220.

[84] Zhang, *How a Tiny Website*, *supra* note 23.

part of"[85] those individuals.[86] As people continue to build out recreational DNA databases, "this newfound tracking capacity [will] run[] against everyone,"[87] because everyone has DNA and everyone has genetic relatives.

Finally, like CSLI, DNA information has a "retrospective quality"[88] that involves exponentially more individuals—some long gone[89]—as massive recreational DNA databases continue to flourish.[90] While one person's CSLI records can tell investigators each place where that person's cell phone was located for the past five years,[91] one person's DNA data can reveal far more about that person themselves and myriad relatives, past and present.[92] Like CSLI, this DNA information is preserved in a database until someone chooses to use it, or one explicitly requests to have it deleted.[93] However, a critical difference is that when investigators access DNA data from these websites, they access a vast wealth of information about countless individuals without any regulation or oversight at all.[94] In *Carpenter*, the Court stressed that "the progress of science has afforded law enforcement a powerful new tool to carry out its important responsibilities. At the same time, this tool risks Government encroachment of the sort the Framers, 'after consulting the lessons of history,' drafted the Fourth

---

[85] *Carpenter*, 138 S. Ct. at 2220.

[86] *See* Stein, *supra* note 16 (explaining that once a person submits her DNA to a recreational service, that person has "made a decision not just for [her]self but for [her] siblings, for [her] distant cousins, people [she does not] even know [she is] related to, for [her] children, for [her] children's children." (quoting Erin Murphy) (internal quotation marks omitted)).

[87] *Carpenter*, 138 S. Ct. at 2218.

[88] *Id.*

[89] *Cf.* Jouvenal, *supra* note 2.

[90] Regalado, *supra* note 13.

[91] *See Carpenter*, 138 S. Ct. at 2218 ("[W]ireless carriers . . . maintain records for up to five years.").

[92] *See supra* Section I.A.

[93] *See* Erin Brodwin, *DNA-Testing Company 23andMe Has Signed a $300 Million Deal with a Drug Giant. Here's How to Delete Your Data If That Freaks You Out*, BUS. INSIDER (July 25, 2018, 5:27 PM), https://www.businessinsider.com/dna-testing-delete-your-data-23andme-ancestry-2018-7. Depending on the genealogy service used, a request to delete DNA information may not be sufficient to entirely remove that information from the database. For example, while 23andMe will discard a consumer's DNA sample, the terms of the consent agreement make it unclear whether a consumer's "raw genetic data" will be discarded. *Id.* Further, while a consumer can delete her DNA results from Ancestry.com, the company will not delete the consumer's genetic data from any research projects the consumer previously opted into. *Id.* Most strikingly, Helix can keep a consumer's DNA "indefinitely." *Id.*

[94] *See* Scutti, *What the Golden State Killer Case Means*, *supra* note 14.

Amendment to prevent."[95] Thus, DNA in recreational databases, like CSLI, is deserving of Fourth Amendment protections. Traditional Fourth Amendment jurisprudence, however, is inadequate to protect this type of information.

II. LACK OF CONSTITUTIONAL AND STATUTORY PROTECTIONS

In the most fundamental way, DNA makes a person who she is. An individual's DNA stores that individual's most personal, private secrets—secrets that even she herself may not be aware of. Among these many secrets is one that connects her to countless genetic relatives, familiar and unfamiliar, past, present, and future.[96] DNA's ability to connect us to so many other individuals in such an intimate way is something that makes DNA particularly unique. However, because DNA is such a distinctive type of information, neither constitutional nor current statutory protections adequately protect the genetic privacy interests implicated by DNA stored in recreational DNA databases.

This Section will describe why current Fourth Amendment jurisprudence is not protective of genetic privacy in commercial DNA databases. First, the Supreme Court has not addressed whether a warrant is necessary before law enforcement obtains DNA information from a recreational DNA database.[97] Further indicating the intrusiveness of familial searching in recreational databases is the fact that a familial search will not necessarily result in a perpetrator's identification; rather, the government utilizes this investigative technique and obtains sensitive personal information without any probable cause to believe that evidence of a crime will be found in a recreational database. Second, current jurisprudence focused on reasonable expectations of privacy does not protect the DNA stored in recreational databases because, due to the nature of DNA, there is a fundamental inability to exclude others from information that may be disclosed by, or may implicate, any number of genetic relatives. Third, using the logic set out in *Carpenter* and highlighting DNA's unique ability to implicate others, the third-party doctrine should not be applied to DNA stored in recreational DNA databases. Finally, consent

---

[95] *Carpenter*, 138 S. Ct. at 2223 (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

[96] *See* Stein, *supra* note 16.

[97] *See* Ford, *supra* note 13; *cf.* Matthew Haag, *FamilyTreeDNA Admits to Sharing Genetic Data With F.B.I.*, N.Y. TIMES (Feb. 4, 2019), https://www.nytimes.com/2019/02/04/business/family-tree-dna-fbi.html; *see also infra* Section II.A.1.

given by customers of recreational DNA services is not truly informed consent, and when one individual consents to participate in these services she effectively gives consent on behalf of all of her past, present, and future genetic relatives. This Section will also describe the current lack of statutory protections for DNA stored in recreational databases, and will underscore how the genetic privacy of individuals whose DNA is stored in CODIS is currently more protected than the genetic privacy of individuals whose DNA is stored in recreational databases, which provide a much more sophisticated and robust set of data.

A. Traditional Fourth Amendment Protections Do Not Reach DNA Stored in Recreational DNA Databases

The Fourth Amendment to the United States Constitution states that "[t]he right of the people to be secure in their persons . . . against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . . ."[98] The purposes of the Fourth Amendment are "to secure 'the privacies of life' against 'arbitrary power' "[99] and " 'to place obstacles in the way of a too permeating police surveillance.' "[100] As technology has progressed into the era of big data and can track, record, and store in the hands of third parties seemingly unlimited information about individuals, how we protect this type of information must be reconsidered. As the Supreme Court noted in *Carpenter*, "the Court is obligated—as '[s]ubtler and more far-reaching means of invading privacy have become available to the Government'—to ensure that the 'progress of science' does not erode Fourth Amendment protections."[101] It is time that the law catches up with DNA technology.

1. Search Warrants and Probable Cause

While law enforcement is typically required to obtain a search warrant supported by probable cause before conducting a search, this constitutional prerequisite does not protect the genetic privacy of individuals whose DNA is stored in recreational DNA databases or whose relatives have submitted their DNA to these

---

[98] U.S. CONST. amend. IV.

[99] *Carpenter*, 138 S. Ct. at 2214 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

[100] *Id.* (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

[101] *Carpenter*, 138 S. Ct. at 2223 (quoting Olmstead v. United States, 277 U.S. 438, 473, 474 (1928) (Brandeis, J., dissenting)).

services. A search under the Fourth Amendment occurs when law enforcement "violates a subjective expectation of privacy that society recognizes as reasonable."[102] In order to conduct a search during a criminal investigation, law enforcement normally must obtain a search warrant based on probable cause.[103] The probable cause requirement demands that police have sufficient information to believe that they will likely find evidence of criminal activity by conducting a search.[104] Probable cause embraces the concepts of "individualized suspicion" and "antecedent justification." The Court in *Carpenter* noted that under the Fourth Amendment, at least some individualized suspicion is required before police may conduct a search.[105] Furthermore, in *Katz v. United States*, the Supreme Court stressed that antecedent justification, or "an objective predetermination of probable cause," is "central to the Fourth Amendment," and that probable cause cannot be justified after a search is complete.[106]

Although the Supreme Court has further held that, subject to limited exceptions,[107] "searches conducted outside the judicial process . . . are per se unreasonable under the Fourth Amendment,"[108] law enforcement currently may legally conduct warrantless familial searching in recreational DNA databases.[109] In *Katz*, the FBI, without a warrant, placed an electronic recording device outside of a public telephone booth where it suspected Katz placed illegal telephone calls during which he would

---

[102] Kyllo v. United States, 533 U.S. 27, 33 (2001).

[103] U.S. CONST. amend. IV.

[104] Brinegar v. United States, 338 U.S. 160, 175–76 (1949) (defining probable cause as "exist[ing] where 'the facts and circumstances within [police officers'] knowledge and of which they had reasonably trustworthy information (are) sufficient in themselves to warrant a man of reasonable caution in the belief that' an offense has been or is being committed" (quoting Carroll v. United States, 267 U.S. 132, 162 (1925))).

[105] *Carpenter,* 138 S. Ct. at 2221.

[106] Katz v. United States, 389 U.S. 347, 358, 359 (1967).

[107] There are seven discrete exceptions to the search warrant requirement. *See Carpenter*, 138 S. Ct. at 2222 (exigent circumstances); Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973) (consent); Riley v. California, 573 U.S. 373, 384 (2014) (search incident to lawful arrest); Carroll v. United States, 267 U.S. 132, 153 (1925) (automobile); Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971) (plain view); Terry v. Ohio, 392 U.S. 1, 27 (1968) (reasonable search for weapons, or *Terry* stops); United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985) (border searches).

[108] *Katz*, 389 U.S. at 357 ("[T]he Constitution requires 'that the deliberate impartial judgment of a judicial officer . . . be interposed between the citizen and the police.' " (quoting Wong Sung v. United States, 371 U.S. 471, 481–82 (1963))).

[109] *See* Ford, *supra* note 13; *cf.* Haag, *supra* note 97.

"transmit[] wagering information" in violation of federal law.[110] The Government argued that these recordings were not obtained in violation of the Fourth Amendment because it had established probable cause and because the surveillance was limited in scope and duration.[111] The Court rejected this argument, however, finding that this was an illegal search under the Fourth Amendment.[112] The Court reasoned that it was not enough "that officers reasonably expected to find evidence of a particular crime and *voluntarily* confined their activities to the least intrusive means consistent with that end,"[113] because this approach left to police discretion whether and how individuals would be protected by the Fourth Amendment.[114] This reasoning, however, has not yet been applied to DNA data stored in recreational databases, which is currently protected by rules formulated by and in the disretion of the businesses themselves.[115] The genetic information stored in these databases is "governed by the same privacy laws applicable to any consumer product company . . . . It doesn't have any additional levels of safety or security,"[116] and law enforcement need not necessarily obtain a search warrant prior to conducting a search in these databases.[117]

---

[110] *Katz*, 389 U.S. at 348.

[111] *Id.* at 354 (noting that the previous investigation conducted by the Federal Bureau of Investigation indicated "a strong probability that [Katz] was using the telephone" for the criminal activity in question and that agents limited their surveillance "to the specific purpose of establishing the contents of [Katz]'s unlawful . . . communications," and thus only surveilled Katz in "brief periods during which he used the telephone booth, and took great care to overhear only the conversations of [Katz] himself").

[112] *Id.* at 358–59.

[113] *Id.* at 356–57 (emphasis added).

[114] *Id.* at 356, 358–59 ("[T]he inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer.").

[115] *See, e.g.*, Bala, *supra* note 25 ("Without guidance from the government on the matter, [the founder of GEDmatch] navigated difficult decisions—such as which types of crimes law enforcement could use the site to try to solve and whether users should have to opt in to or opt out of sharing their data with the police. . . . [O]ne individual had the power both to draw th[e] line[s] and to change [them] unilaterally. With no legal regulations providing clarity on how and when genetic genealogy should be used to fight crime, we have left private entities in charge of the decision-making.").

[116] Scutti, *What the Golden State Killer Case Means*, *supra* note 14 (internal quotation omitted).

[117] *See* Ford, *supra* note 13; *cf.* Haag, *supra* note 97.

While some recreational genealogy companies have voluntarily chosen to include such protections in their privacy policies, such protection is woefully insufficient.[118] Services like AncestryDNA and 23andMe have stated that they will only share information with law enforcement if it is legally compelled.[119] However, their privacy policies appear to leave discretion to the companies themselves regarding when to share this information. For example, AncestryDNA's Privacy Statement states that Ancestry DNA "may share [a customer's] Personal Information *if we believe* it is reasonably necessary to . . . [c]omply with valid legal process (e.g., subpoenas, warrants)."[120] 23andMe's Privacy Statement states that "23andMe will preserve and disclose any and all information to law enforcement agencies or others if required to do so by law *or in the good faith belief* that such preservation or disclosure is reasonably necessary to . . . comply with legal or regulatory process . . . ."[121] Conversely, GEDmatch requires no warrant at all[122] and is very upfront in its Terms of Service and Privacy Policy, explicitly informing its users that if they "require absolute privacy and security" they should not provide their information to GEDmatch at all, or should "delete it immediately" if they have already provided it.[123]

---

[118] Brown, *supra* note 19 ("The only rules [about familial searching in the consumer space] are in each company's terms of service. Even then, there may be little a company can realistically do to keep law enforcement agencies—or anyone else—from using its service however they like.").

[119] *See* Jouvenal, Berman, Harwell & Jackman, *supra* note 22. Regardless of how protective recreational genealogy services choose to make their privacy policies, a recent ruling in Florida paves the road for law enforcement's unfettered use of DNA stored in recreational databases. In July 2019, Judge Patricia Strowbridge of the Ninth Judicial Circuit Court of Florida approved a detective's request for a search warrant to allow him to "override the privacy settings of GEDmatch's users and search the site's full database." Kashmir Hill & Heather Murphy, *Your DNA Profile is Private? A Florida Judge Just Said Otherwise*, N.Y. TIMES (Nov. 5, 2019), http://www.nytimes.com/2019/11/05/business/dna-database-search-warrant.html. Within twenty-four hours, GEDmatch complied with the warrant. *Id.* Thus, there now exists precedent for future investigators to obtain similar warrants to search within even larger databases, like AncestryDNA and 23andMe. *Id.* (highlighting concern among DNA policy experts that such precedent may transform "all genetic databases into law enforcement databases").

[120] *Privacy Statement*, ANCESTRYDNA, https://www.ancestry.com/cs/legal/privacystatement (last updated Dec. 23, 2019) (emphasis added).

[121] *Privacy Statement*, 23ANDME, https://www.23andme.com/about/privacy/ (last updated Jan. 1, 2020) (emphasis added).

[122] *See* Ford, *supra* note 13 (explaining that GEDmatch, an "open-source system[,] allowed investigators to avoid the need for a warrant").

[123] *GEDmatch.com Terms of Service and Privacy Policy*, GEDMATCH, https://www.gedmatch.com/tos.htm (last updated Dec. 9, 2019). On May 18, 2019,

Additionally, "[m]any commercial genetic testing company contracts with participants 'have clauses that allow them to change their policy as they choose,' "[124] which underscores the fact that this highly sensitive information is not protected in a dependable way. Even companies that tout their commitment to consumer privacy may choose at any time to allow investigators to

GEDmatch updated its terms and service to clarify that it accepts law enforcement's use of its service for familial search purposes. *Id.* ("When you upload Raw Data to GEDmatch, you agree that the Raw Data is one of the following: . . . DNA obtained and authorized by law enforcement to identify a perpetrator of a violent crime against another individual . . . .; [or] DNA obtained and authorized by law enforcement to identify remains of a deceased individual."). At that time, GEDmatch also added a "Public + opt-out" feature, allowing individuals' DNA to be "available for comparison to any Raw Data in the GEDmatch database, except DNA kits identified as being uploaded for Law Enforcement purposes." *Id.* One week later, GEDmatch updated its privacy policy again, this time implementing an opt-in option for users to select in order to allow law enforcement to utilize their DNA. Natalie Ram, *The Genealogy Site that Helped Catch the Golden State Killer is Grappling with Privacy*, SLATE (May 29, 2019, 7:30 AM), https://slate.com/technology/2019/05/gedmatch-dna-privacy-update-law-enforcement-genetic-geneology-searches.html (last visited Jan. 20, 2020). Alarmingly, Verogen, Inc., a "forensic genomics company whose focus is on human ID," announced on December 9, 2019 that it had purchased GEDmatch. Email from Curtis Rogers, Founder, GEDmatch, to Jamie Zeevi/GEDmatch users (Dec. 19, 2019, 10:09 PM EST) (on file with author) [hereinafter GEDmatch Email]. Verogen, Inc. openly views GEDmatch as not only a recreational DNA database, but as a valuable resource for law enforcement. *Id.* ("Verogen recognizes that law enforcement use of genetic genealogy is here to stay . . . ."); *see also* Bala, *supra* note 25 (noting that Verogen is currently cooperating with the FBI to "create DNA profiles for the National DNA Index System," that Verogen's Chief Operating Officer has stated that he views GEDmatch as "molecular eyewitness" that can be used by law enforcement as a tool to solve crimes, and that "selling its services to crime labs" is "explicitly" part of Verogen's business model). Thus, it appears that GEDmatch is more committed than ever to cooperating with and assisting law enforcement.

[124] Scutti, *What the Golden State Killer Case Means*, *supra* note 14; *see Privacy Statement*, ANCESTRY, https://www.ancestry.com/cs/legal/privacystatement (last updated Dec. 23, 2019) ("We may modify this Privacy Statement at any time . . . ."); *Privacy Statement*, 23ANDME, https://www.23andme.com/about/privacy/ (last updated Jan. 1, 2020) ("Whenever this Privacy Statement is changed in a material way, a notice will be posted . . . -[and] [a]fter 30 days the changes will become effective."); *GEDmatch.com Terms of Service and Privacy Policy*, GEDMATCH, https://www.gedmatch.com/tos.htm (last updated Dec. 9, 2019) ("We may update the GEDmatch.Com Terms of Service and Privacy Policy at any time."). For a detailed history of past changes made to GEDmatch's privacy policy, see Bala, *supra* note 25. When Verogen, Inc. purchased GEDmatch, it committed to "fight all unauthorized law enforcement use and any warrants that may be issued," GEDmatch Email, *supra* note 123, and announced that "GEDmatch's terms of service will not change, with respect to the use, purposes of processing, and disclosures of user data." Julian Husbands, *GEDmatch Partners with Genomics Firm*, Verogen (Dec. 9, 2019), https://www.verogen.com/gedmatch-partners-with-genomics-firm/ (last visited Jan. 20, 2020). However, there is nothing to prevent Verogen from changing GEDmatch's policies in the future. Bala, *supra* note 25.

access their databases and even utilize their laboratories. In 2018, for example, FamilyTreeDNA, a company that had actively "marketed itself as a leader of consumer privacy and a fierce protector of user data" voluntarily allowed the FBI to access its DNA databases and to utilize its laboratory for investigations of unsolved violent crimes without ever notifying its users.[125] It became "the first known commercial site to provide some services without a subpoena or warrant,"[126] as opposed to GEDmatch, which is a free, open-source website.[127] There is currently no legal reason other such commercial sites would not do the same. Because there is little uniformity amongst recreational genealogy companies' privacy policies, and because these companies retain the power to change these policies at any time, discretion is in the hands of these companies whether and how to protect the genetic privacy of their users and, by extension, that of their users' genetic relatives. Like in *Katz*, where the Court rejected the self-restraint argument presented by the Government and deemed a warrantless search unconstitutional,[128] searches within recreational DNA databases must require more stringent legal protection.

Furthermore, when conducting a familial search in a recreational DNA database, law enforcement does so without the need to establish probable cause. In fact, law enforcement engages in this investigative technique precisely because it cannot establish probable cause with respect to an individual. When investigators conduct such a search, they are inputting DNA from a crime scene in hopes, but with no guarantee, that a partial match will be made. In this context, while this genetic information is being used in a criminal investigation, it will not provide evidence of criminal activity; at most, it will provide law enforcement with leads.[129] Probable cause requires more than this. Before law enforcement conducts a familial search, it has no indication whether the search will result in a partial match at all. Thus, it would be nearly impossible to argue that law enforcement would be able to demonstrate probable cause to conduct such a search.

---

[125] Haag, *supra* note 97. This did not become public until 2019. *Id.*

[126] *Id.*

[127] *See* Zhang, *How a Tiny Website*, *supra* note 23; Ford, *supra* note 13.

[128] Katz v. United States, 389 U.S. 347, 358–59 (1967).

[129] *See* Eli Rosenberg, *Family DNA Searches Seen as Crime-Solving Tool, and Intrusion on Rights*, NY TIMES (Jan. 27, 2017), https://www.nytimes.com/2017/01/27/nyregion/familial-dna-searching-karina-vetrano.html.

Finally, familial searching in recreational databases casts a wide net that drags in myriad, presumptively innocent, individuals who were never subject to any individualized suspicion whatsoever. Essentially, law enforcement is sifting through the DNA and genealogy of countless random individuals who are distantly related to a perpetrator whose identity they do not know. This cannot meet the individualized suspicion requirement. Nevertheless, the intimate information of these individuals is utilized in criminal investigations without any legal or judicial oversight. This is more akin to a fishing expedition than a search with a reasonably limited scope and reasonably likely results. Familial searching in recreational DNA databases, it seems, is the "too permeating police surveillance"[130] that the Fourth Amendment was designed to protect against.

2. Reasonable Expectation of Privacy

Due to the unique nature of DNA, current reasonable expectation of privacy jurisprudence provides an insufficient standard to protect the DNA stored in recreational databases. "[T]he protections of the Fourth Amendment are activated only when the state conducts a search or seizure in an area in which there is a 'constitutionally protected reasonable expectation of privacy.' "[131] Fourth Amendment jurisprudence has recognized two requirements that must be fulfilled in order for a reasonable expectation of privacy to be established: where an individual seeks to preserve things as private and where the subject is something society is reasonably prepared to recognize as private.[132] "When there is no reasonable expectation of privacy," however, "the Fourth Amendment is not implicated."[133]

In determining whether a person has a reasonable expectation of privacy, the Supreme Court has often highlighted the importance of one's ability to exclude others in order to preserve one's privacy. In *Katz*, the Court explained that a person may have

---

[130] Carpenter v. United States, 138 S. Ct. 2206, 2214 (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

[131] United States v. Davis, 690 F.3d 226, 241 (4th Cir. 2012) (quoting New York v. Class, 475 U.S. 106, 112 (1986)).

[132] *Carpenter*, 138 S. Ct. at 2213 ("When an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable,' we have held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause." (quoting Smith v. Maryland, 442 U.S. 735, 740 (1979))).

[133] *Davis*, 690 F.3d at 241.

a reasonable expectation of privacy in that which she "seeks to preserve as private" not only in her own home, but "even in an area accessible to the public."[134] In addition, the Court in *Rakas v. Illinois* explained that having a reasonable expectation of privacy is not always a function of having a proprietary interest, but may also exist where an individual has a "sufficient interest" in, and the ability to exclude others from, that which she seeks to preserve as private.[135] In *Rakas*, the Court reiterated the reasoning in *Katz* that the "capacity to claim the protection of the Fourth Amendment depends not upon a property right in the invaded place but upon whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place."[136] The Court in *Rakas* determined that the defendants did not have a reasonable expectation of privacy in the particular places in which a car was searched, not only because they owned neither the car nor the items seized, but also because the glove compartment and areas under the seats are not places in which passengers would "normally have a legitimate expectation of privacy."[137] In its reasoning, the Court contrasted the facts of *Rakas* with those of *Jones*, where "Jones had complete dominion and control over the apartment and could exclude others from it," and those of *Katz*, where Katz was able to close the door to the telephone booth "to exclude all others."[138] The Court's juxtaposition and comparison of the facts of these three cases reiterates the importance of a person's ability to exclude others to whether that person has a reasonable expectation of privacy.

---

[134] Katz v. United States, 389 U.S. 347, 351–52 (1967) (holding that Katz had a reasonable expectation of privacy in a telephone booth because he "occupie[d] it, shut[] the door behind him, and pa[id] the toll that permit[ted] him to place a call").

[135] Rakas v. Illinois, 439 U.S. 128, 142 (1978). The *Rakas* Court illustrated this using the facts of *Jones v. United States* as an example, where Jones was held to have a reasonable expectation of privacy in a friend's apartment where he was staying, when "[t]he friend had given him permission to use the apartment and a key to it." *Id.* at 141 (citing Jones v. United States, 362 U.S. 257, 259 (1960)).

[136] *Id.* at 143. In *Rakas*, police seized a sawed-off rifle and shells, which the defendants did not own, from the glove compartment and under the seats of a car, which the defendants were passengers in but did not own. *Id.* at 129.

[137] *Id.* at 148–49.

[138] *Id.* at 149.

Although society has long recognized that people have a reasonable expectation of privacy in their bodies,[139] Fourth Amendment reasonable expectation of privacy precedent does not map onto DNA in recreational DNA databases. In 2012, the Fourth Circuit in *United States v. Davis* took a step forward in establishing that a person has a reasonable expectation of privacy in the information that her own DNA may provide, due to the ability of DNA to reveal deeply private information about that person.[140] However, this precedent does not go far enough in protecting DNA in recreational databases. Even if a person affirmatively chooses not to submit her DNA to a recreational database in order to exclude others and to maintain her genetic privacy, she has no control over whether a distant relative will reveal portions of this information on her behalf.[141] Furthermore, the law is murky when it comes to whether a genetic relative may claim a reasonable expectation of privacy in the DNA of another genetic relative. While a substantial amount of case law has defined the contours of the reasonable expectation of privacy in different scenarios, the same cannot be said for DNA, which may involve relatives regardless of whether they have chosen to preserve their own DNA as private.

An additional wrinkle in Fourth Amendment reasonable expectation of privacy jurisprudence is that an individual's reasonable expectation of privacy is diminished when she is arrested.[142] *Maryland v. King*, decided by the Supreme Court in 2013, addressed the issue of whether it is a Fourth Amendment violation for law enforcement, without a warrant, to collect and analyze DNA from persons arrested on felony charges but not yet convicted.[143] The Court held that in this context, obtaining an

---

[139] United States v. Davis, 690 F.3d 226, 243 (4th Cir. 2012) ("[B]ecause the analysis of biological samples . . . can reveal 'physiological data' and a 'host of private medical facts,' such analyses may 'intrude[] upon expectations of privacy that society has long recognized as reasonable.' " (quoting Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 616–17 (1989)).

[140] *Id.* at 243–44.

[141] *See* Murphy, *supra* note 36, at e8 ("[T]he fact that a fifth cousin once removed uploaded their DNA to an online site means that the government still has one's profile, anyway.").

[142] Maryland v. King, 569 U.S. 435, 462–63 (2013) ("The expectations of privacy of an individual taken into police custody 'necessarily [are] of a diminished scope.' . . . [U]nlike the search of a citizen who has not been suspected of a wrong, a detainee has a reduced expectation of privacy." (quoting Bell v. Wolfish, 441 U.S. 520, 557 (1979)).

[143] *Id.* at 442.

arrestee's DNA as a "part of a routine booking procedure" is reasonable and does not require a warrant.[144] Comparing this practice to photographing or fingerprinting arrestees,[145] the Court reasoned that arrestees "in valid police custody for . . . serious offense[s] supported by probable cause" have a decreased expectation of privacy that is outweighed by the government's legitimate interest in safely and accurately identifying people in its custody.[146]

Unlike DNA samples collected from arrestees, the DNA contained in recreational databases is voluntarily provided by free individuals who submitted their DNA samples to these websites. We must presume that at least some individuals who affirmatively choose not to submit their DNA, but are genetically related to individuals who do, are free individuals. In this context, it is the general public that is affected, not a subgroup of individuals who may have a diminished expectation of privacy due to contact with the criminal justice system. Thus, the reasonable expectation of privacy that free individuals have in their DNA is undermined by its use in criminal investigations without legal protection.

Furthermore, the court in *Davis* was careful to clarify that even a victim of a crime, whose DNA "has come into the lawful possession of the police," maintains a reasonable expectation of privacy in her DNA.[147] The court expressed concern that such citizens would "lose any expectation of privacy in [their DNA], which could be used against [them] at a later date without the constitutional safeguard that a warrant supported by probable cause first be issued."[148] Just as the *Davis* court was concerned with protecting this type of information when it came to free individuals in the criminal context, this concern for protection must be expanded to DNA in the recreational context as well.

Additionally, there is a general sense in society that DNA should be recognized as something private, and thus protected by the Fourth Amendment.[149] While traditional Fourth Amendment jurisprudence deals mainly with physical spaces and property and not the more abstract and intangible type of information that DNA is and how it can be accessed, in the context of DNA in recreational

---

[144] *Id.* at 465–66.
[145] *Id.* at 451.
[146] *Id.* at 448, 449.
[147] United States v. Davis, 690 F.3d 226, 244 (4th Cir. 2012).
[148] *Id.*
[149] *See* Jouvenal et al., *supra* note 22.

databases the Supreme Court's judicious words in 1925 remain relevant today: "The Fourth Amendment is to be construed . . . in a manner which will conserve public interests as well as the interests and rights of individual citizens."[150] Because the DNA in recreational DNA databases, as compared to the DNA in CODIS, has the ability to provide an enormous amount of personal and intimate information about individuals,[151] DNA in these databases must be protected from uninhibited use by law enforcement in criminal investigations. DNA is different in that while there is a feeling in society that this type of information is deserving of privacy protections, there is simultaneously a fundamental inability to exclude others from revealing this information. Because current Fourth Amendment jurisprudence regarding the reasonable expectation of privacy does not protect DNA stored in recreational DNA databases, and because it does not protect individuals genetically related to individuals in such databases, statutory protections are necessary to allow individuals to exclude others in a way that people are not currently capable of doing themselves.

3. Third-Party Doctrine

The third-party doctrine provides that when a person voluntarily gives her information to a third-party, she no longer has a reasonable expectation of privacy in that information, "even if the information is revealed on the assumption that it will be used only for a limited purpose."[152] The government may thus access this information without concern for Fourth Amendment protections.[153] In *Carpenter*, the Supreme Court considered the limits of the third-party doctrine in light of modern technology, and determined that due to the extensive and revealing nature of CSLI information and the fact that it is automatically collected, the third-party doctrine did not override the need for Fourth Amendment protection.[154] The Court explained that, because cell phones are "indispensable to participation in modern society," and because CSLI records are created automatically when a cell phone is operated, CSLI is "not truly

---

[150] Carroll v. United States, 267 U.S. 132, 149 (1925).

[151] *See* Murphy, *supra* note 36, at e5.

[152] Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) (quoting United States v. Miller, 425 U.S. 435, 443 (1976)).

[153] *Id.*

[154] *Id.* at 2223.

'shared' as one normally understands the term."[155] Thus, the Court reasoned, "in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements."[156]

Similarly, due to the extensive and revealing nature of the DNA data provided to recreational databases, Fourth Amendment protections should override the third-party doctrine. First, although individuals voluntarily submit their DNA to these services, the information is provided for limited purposes. Although alone, this is not enough to override the third-party doctrine, the extent of what DNA may reveal about an individual, together with the likelihood that individuals who submit their DNA samples do not fully understand what they are providing, demonstrates the need for additional protection. The Court conceded in *Carpenter* that its interpretation and application of the third-party doctrine "must take account of more sophisticated [technology] that [is] already in use or in development."[157] The rapidly evolving study of what DNA can reveal must be taken into account when considering the level of protection it receives.

Second, DNA is different from CSLI due to its unique ability to implicate genetic relatives, which creates what has been called a "fourth-party problem."[158] Fourth parties are those who have not submitted their own DNA samples, but are genetically related to people who have, and can thus be pulled into criminal investigations anyway. Put simply, "[i]f you're upset that your brother has uploaded his DNA to a commercial DNA database . . . you don't really have any legal rights to complain if the police decide, for example, to collect that DNA or to analyze it or take a look at it."[159] These individuals do not fall into the category of individuals subject to the third-party doctrine, nor do Fourth Amendment protections adequately protect their reasonable expectations of privacy in their own DNA. Because DNA is different, these people fall through the cracks between legal protections. A person "shouldn't have fewer civil rights because [she is] related to someone who broke the law."[160]

---

[155] *Id.* at 2220.
[156] *Id.* (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979)).
[157] *Id.* at 2218 (quoting Kyllo v. United States, 533 U.S. 27, 36 (2001)).
[158] Ford, *supra* note 13.
[159] *Id.*
[160] Rosenberg, *supra* note 129.

4. Consent

While a warrantless search may be constitutional under the Fourth Amendment if the person being searched consents to it,[161] consent is not a valid argument in the context of DNA in recreational databases. First, the consent given by users of these genealogy services is not truly informed consent. Second, even if an individual does give fully informed consent, she is effectively giving this consent on behalf of all her genetic relatives. Similarly, the option to opt out of allowing one's DNA to be used in forensic investigations is insufficient due to the ability of another genetic relative to opt in.

Consent given by individuals who submit their DNA to recreational databases is not truly informed consent.[162] The consent that individuals provide is often hidden deep in the fine print of the terms and conditions of these services.[163] Even if a person takes the time to read the entirety of the terms and conditions, that person may not understand the extent of what she has consented to and what the agreement will allow the company to do with her DNA.[164] Those who submit their information to recreational DNA databases to learn more about their own genealogy or health predispositions likely have not fully contemplated, nor do they fully understand, the extent of what their DNA may reveal or how it can be used now or in the future.[165] Individuals likely do not have a true understanding of "the downstream applications of their pooled genetic profiles," and the implications of "third-party access" to this information.[166] Additionally, the privacy statements and the terms and conditions

---

[161] Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973).

[162] *See* Kimberlee Sue Moran, *Damned By DNA – Balancing Personal Privacy With Public Safety*, 292 FORENSIC SCI. INT'L e3, e4 (2018).

[163] *Id.*

[164] Maggie Fox, *What You're Giving Away with Those Home DNA Tests*, NBC NEWS (Nov. 29, 2017, 6:16 PM), https://www.nbcnews.com/health/health-news/what-you-re-giving-away-those-home-dna-tests-n824776.

[165] Scutti, *What the Golden State Killer Case Means*, *supra* note 14.

[166] Moran, *supra* note 162, at e4. For example, 23andMe shares this information with "academic and industry partners" for medical research purposes and "cannot guarantee what will happen to the information once it leaves their hands." Scutti, *What the Golden State Killer Case Means*, *supra* note 14; *see also* Rubén Rosario, Opinion, *Rosario: Familial DNA Searches Are Becoming a Useful Cop Tool in Cold Cases*, PIONEER PRESS (Mar. 1, 2019, 12:01 PM), https://www.twincities.com/2019/03/01/rosario-familial-dna-searches-are-becoming-a-useful-cop-tool-in-cold-cases/ ("I was wary of giving out my DNA. I did it anyway. But most of us really don't know how accessible our genetic profiles, and, indirectly, those of family members, might be to third parties, including the government, by willingly using these sites.").

of use of recreational DNA services is often very broad and subject to change at any time.[167] Thus, "[w]ithout greater transparency about the number and nature of recreational genetic searches, it is impossible for the public to reach an informed decision about their permissible scope."[168]

In the context of DNA, individuals have the unique ability to essentially, and likely unknowingly, disclose the genetic relationships between themselves and their genetic relatives on behalf of their genetic relatives. Simply requiring a party's consent to access her DNA data does not address the issue because the privacy rights of relatives are automatically compromised by access to the data. When an individual gives consent to recreational DNA databases to use her DNA, "[s]uch consent is not limited to the individual user's DNA. It extends to everyone who shares that genetic information—past, present, and future."[169] Critically, when people consent to sharing their DNA with such a service, it is unlikely that they are considering "the genetic privacy of their distant relatives."[170] Moreover, it is highly unlikely that before consenting to the use of their DNA by commercial genealogy services, consumers considered the possibility that "intimate pieces of their DNA" could be utilized by law enforcement in criminal investigations.[171] Individuals are generally accustomed to having a choice in whether and when to share their private information with others. After all, the information is private. DNA, however, is different.

Some may argue that providing users of recreational DNA databases with an opt-out option resolves the issue of informed consent. The argument would be that providing an opt-out option restores users' ability to give informed consent by choosing not to delete their genetic information and profiles from databases once they learn that their data may be used in ways not originally contemplated, like in criminal investigations.[172] This argument,

---

[167] *See supra* Section II.A.1.

[168] Murphy, *supra* note 36, at e7.

[169] Moran, *supra* note 162, at e4.

[170] Ritter, *supra* note 19.

[171] Kolata & Murphy, *supra* note 1. "[N]o consent has been given by the contributors to a genealogical collection for their DNA to be used in a way that might implicate their relatives in a committed crime." Denise Syndercombe Court, *Forensic Genealogy: Some Serious Concerns*, 36 FORENSIC SCI. INT'L: GENETICS 203, 203 (2018).

[172] Soon after the arrest of the Golden State Killer, GEDMatch highlighted an opt-out option for its users, posting the following announcement on the GEDMatch website:

however, completely ignores DNA's unique ability to implicate one's relatives and thus does not solve the nonconsent issue. The issue remains that the decision to maintain one's genetic privacy is not in the hands of that individual. Even if a person makes the decision to delete her DNA data that she had once submitted to a recreational database, she cannot be guaranteed that any of her relatives who submitted their DNA would make the same decision.[173] Furthermore, a person who never submitted her own DNA in the first place cannot be guaranteed that her relatives would choose to opt out. In both situations, individuals who chose to maintain their genetic privacy are implicated regardless of their personal decisions, and the power to consent to a potential genetic privacy waiver remains with someone else.

Stated another way, one person's DNA submission to a recreational DNA database may effectively serve as a waiver of that person's individual privacy in her own DNA, as well as that of countless others who may have otherwise chosen to keep this information private.[174] It is becoming ever more likely that any given person will have at least a distant relative in "a publicly searchable database."[175] Critically, even if individuals consent to waiving their privacy interest in their DNA, "they're also [consenting for] their extended family, their children, [and] their children's children. . . . And they're not just [consenting] for" the present year, but for years in the future as well, "when data from the genome could be used in all sorts of different ways."[176] "The reckless handover of DNA erodes our ability to collectively protect our personal privacy and violates the privacy of those genetically related but who have not given their explicit consent to be included in a database."[177]

> While the database was created for genealogical research, it is important that GEDmatch participants understand the possible uses of their DNA, including identification of relatives that have committed crimes or were victims of crimes. If you are concerned about non-genealogical uses of your DNA, you should not upload your DNA to the database and/or you should remove DNA that has already been uploaded.

Kolata & Murphy, *supra* note 1.

[173] Molteni, *supra* note 12 ("You can't claw back the profile of your third cousin once removed who you don't even know exists." (internal quotation omitted)).

[174] Kolata & Murphy, *supra* note 1 ("Suppose you are worried about genetic privacy. . . . If your sibling or parent or child engaged in this activity online, they are compromising your family for generations.").

[175] Ritter, *supra* note 19.

[176] Jouvenal et al., *supra* note 22.

[177] Moran, *supra* note 162, at e4.

B. *No Statutory Protections Exist for DNA Stored in Recreational DNA Databases*

The Genetic Information Nondiscrimination Act of 2008 went into effect on May 21, 2008.[178] The purpose of this Act was "[t]o prohibit discrimination on the basis of genetic information with respect to health insurance and employment."[179] In making the determination that this Act was necessary to protect individuals from the potential consequences of scientific progress, Congress recognized that the advances in genetic science and testing may "give rise to the potential misuse of genetic information to discriminate in health insurance and employment."[180] While some argue that this Act may not have gone far enough to protect individuals from genetic discrimination, it provides no protection whatsoever for DNA in recreational databases.[181] Just as there are protections regarding the provision of this type of information to doctors and health insurance companies, protections regarding law enforcement's access to and use of this type of information must be protected as well.

While some statutes do exist to protect the DNA information stored in CODIS and to regulate how such information may be used, these regulations vary widely. For example, "[w]hile familial searching is not performed at the national level,"[182] states differ as to whether they use familial searching at all and as to what limits are placed on the practice. Currently, only a number of states allow familial searching: Arizona, Arkansas, California, Colorado, Florida, Michigan, Minnesota, New York, Ohio, Texas, Utah, Virginia, Wisconsin, and Wyoming.[183] While Illinois and

---

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

[179] *Id.*

[180] Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, § 2, 122 Stat. 881 (2008).

[181] Scutti, *What the Golden State Killer Case Means*, *supra* note 14 ("[T]he act does not apply to companies with fewer than 15 employees, and 'other forms of insurance including life, disability and long-term care are not covered by [the Genetic Information Nondiscrimination Act].' " (quoting Jeremy Gruber)).

[182] Combined DNA Index System (CODIS), FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis (last visited Oct. 18, 2019).

[183] James Rainey, *Familial DNA Puts Elusive Killers Behind Bars. But Only 12 States Use It.*, NBC NEWS (Apr. 18, 2018, 6:00 AM), https://www.nbcnews.com/news/us-news/familial-dna-puts-elusive-killers-behind-bars-only-12-states-n869711; Combined DNA Index System (CODIS), FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis (last visited Oct. 18, 2019).

Louisiana are currently considering whether to allow familial searching in CODIS, Maryland and Washington D.C. have chosen not to allow the use of this technique at all.[184] However, while minimal regulations protect DNA information in CODIS, there are currently no laws regulating familial searching using recreational DNA websites.[185]

As the DNA testing that is currently performed by recreational DNA services is "more sophisticated than the DNA tests police currently run, and . . . generate[s] more data than is stored in the FBI's CODIS database," this lack of statutory protection is, at the very least, alarming.[186] "[S]earches in recreational databases affect a far greater number of innocent persons, and are conducted with no oversight or governance of any kind."[187] Strikingly, the STR-tested DNA in CODIS, collected from individuals with a decreased expectation of privacy, is more protected than the SNP-tested DNA of innocent individuals in the recreational context.[188]

For example, a number of simple regulations exist for laboratories conducting searches in CODIS, which "represent an effort to balance the right of individuals to genetic privacy, and to be free from government intrusion in the absence of suspicion, against the desire to apprehend law breakers."[189] Such regulations include requirements that "[a]ll genetic material tested for upload into the database . . . be done by accredited laboratories and qualified personnel," that any DNA sample submitted must be from "a 'putative perpetrator' . . . [and not] profiles derived from evidence that may [only] have a remote connection to the crime, or from a mere witness or bystander."[190]

---

[184] Rainey, *supra* note 183.

[185] Murphy, *supra* note 36, at e6. In January 2019, Maryland legislators introduced a bill that seeks to extend the state's ban on familial searching in CODIS to cover consumer genetic databases as well. Natalie Jones, *Maryland Bill Seeks to Prohibit Using DNA Databases to Solve Crime*, NBC WASH. (Feb. 21, 2019, 7:22 AM), https://www.nbcwashington.com/news/local/Bill-Seeks-to-Prohibit-Using-DNA-Databases-to-Solve-Crime-506147871.html. As of this writing, the bill remains adjourned *sine die*. Maryland House Bill 30, LEGISCAN, https://legiscan.com/MD/bill/HB30/2019 (last visited Sep. 17, 2019).

[186] Zhang, *The Coming Wave of Murders Solved*, *supra* note 12.

[187] Murphy, *supra* note 36, at e5.

[188] *See id.* at e7.

[189] *Id.* at e6.

[190] *Id.*

In addition to regulating the use of CODIS, jurisdictions that allow for familial DNA searches often "supplement these requirements with [additional] policies."[191] Some limits that have been enacted include only permitting familial searching to be used "to solve the most serious cases," and establishing "[a] separate oversight committee [to] determine[] when a familial match is strong enough to disclose it to local investigators."[192] Some policies also require "that any incidental findings (e.g., non-paternity) are distanced from local law enforcement," and that "[w]innowing of leads" be accomplished "through public or police resources, so as to minimize the intrusion on persons ultimately ruled out as a potential lead or suspect."[193]

In stark contrast, no such regulations exist surrounding the use of familial searching in recreational DNA databases.[194] This currently provides law enforcement with the ability to conduct in recreational databases the searches that they are prohibited from conducting in CODIS.[195] For example, there are no laws or regulations currently preventing law enforcement from engaging in "fishing expedition[s]" to find not only perpetrators of crimes, but individuals tangentially related to the crimes.[196] And once individuals are pinpointed, there are no current laws regulating the types of follow-up investigations that law enforcement may conduct.[197] "[A] genealogical detective," for example, "can take endless amounts of surreptitious samples, . . . [and] sneak sampl[e] persons in the 'family tree' even though they are *not* suspects, simply because such samples might help expedite the investigation by eliminating potential suspect 'branches.' "[198] The result of this regulatory imbalance is simple and nonsensical—"the immediate sibling of a convicted offender

---

[191] *Id.*

[192] *Id.* (referencing policies adopted in California).

[193] *Id.* (referencing policies adopted in California).

[194] *Id.*

[195] *Id.* at e7.

[196] *Id.* at e6. This technique may currently be used not only to identify perpetrators, but "victims, witnesses, [and] bystanders" as well. *Id.*

[197] *Id.*

[198] *Id.* In the search for the Golden State Killer, police surreptitiously collected DNA samples from two individual suspects who turned out to be innocent. *Id.* "Samples could . . . be taken from victims, victims' family members or loved ones, or purported witnesses to a crime—all without those persons knowing that they had been targeted by police." *Id.* at e6–e7.

has greater protection against genetic surveillance . . . than a distant biological relation of a person interested in recreational genomics."[199]

III. COMMON COUNTERARGUMENTS AND WHY THEY ARE FLAWED

A. The Government's Interest in Identifying Criminals Does Not Completely Outweigh the Individual's Interest in Genetic Privacy

The government has a strong interest in identifying criminals for the dual purposes of apprehending them and preventing future crimes, and many argue that this government interest outweighs the interest of the individual in maintaining her genetic privacy. In *Maryland v. King*, police took a DNA sample from King "[a]s part of a routine booking procedure for serious offenses," and his DNA was later found to be a match to DNA obtained from a rape victim in an unrelated case.[200] Holding that "DNA identification of arrestees is a reasonable search that can be considered part of a routine booking procedure,"[201] the Supreme Court recognized the government's strong interest in identification as it pertains to persons in custody and analogized the use of DNA for identification purposes to law enforcement's use of fingerprinting.[202] The Supreme Court reasoned that DNA, like a fingerprint, can provide "an irrefutable identification of the person from whom it was taken," and that neither fingerprints nor DNA are "themselves evidence of any particular crime."[203] The Court further explained that because law enforcement already uses routine techniques like fingerprinting and utilization of mug shots to identify individuals, "[t]he only difference between DNA analysis and the accepted use of fingerprint databases is the unparalleled accuracy DNA provides."[204]

---

[199] *Id.* at e7.

[200] Maryland v. King, 569 U.S. 435, 440 (2013).

[201] *Id.* at 465.

[202] *Id.* at 449, 451.

[203] *Id.* at 451.

[204] *Id.* at 436, 451 ("A DNA profile is useful to police because it gives them a form of identification to search the records already in their valid possession. In this respect the use of DNA for identification is no different than matching an arrestee's face to a wanted poster of a previously unidentified suspect . . . or matching the arrestee's fingerprints to those recovered from a crime scene.").

Outstandingly, the Court overlooked the essential feature of DNA—the vast wealth of information it contains—and failed to take into consideration this fundamental difference between DNA and other identification techniques, like fingerprinting. It would be difficult to overstate how much more revealing DNA data is than a fingerprint. Neither a fingerprint nor a mug shot has the capability of doing much more than assisting law enforcement in confirming the identify of a single individual. In contrast, even in the criminal context, the STR DNA used in CODIS has the ability to reveal more, with the potential to point to a person's immediate relatives.[205] This is not to mention the myriad details that the SNP DNA stored in recreational DNA databases can reveal about an individual and her extended relatives.[206] Furthermore, modern genetic science likely has not scratched the tip of the iceberg in determining what SNP DNA, or even what we currently dub "junk DNA," may be able to reveal.[207]

Regardless, the Court's logic has not been extended to law enforcement's use of recreational DNA databases to conduct such searches, especially when the search is conducted without individualized suspicion. When there is such a lack of individualized suspicion, the Supreme Court has noted that "the reasonableness of a search 'is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's [reasonable expectation of] privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental

---

[205] *See supra* Section I.A.

[206] *See supra* Section I.A.

[207] *See, e.g.*, *What are the Next Steps in Gemonic Research?*, NAT'L INST. HEALTH (Jan. 7, 2020), https://ghr.nlm.nih.gov/primer/genomicresearch/nextsteps (last visited Jan. 13, 2020) ("Discovering the sequence of the human genome was only the first step in understanding how the instructions coded in DNA lead to a functioning human being. The next stage of genomic research will begin to derive meaningful knowledge from the DNA sequence. Research studies that build on the work of the Human Genome Project are under way worldwide."); *see also, e.g.*, *What is the Encyclopedia of DNA Elements (ENCODE) Project?*, NAT'L INST. HEALTH (Jan. 7, 2020), https://ghr.nlm.nih.gov/primer/genomicresearch/encode (last visted Jan. 13, 2020) ("The approximately 20,000 genes that provide instructions for making proteins account for only about 1 percent of the human genome. Researchers embarked on the ENCODE Project to figure out the purpose of the remaining 99 percent of the genome. Scientists discovered that more than 80 percent of this non-gene component of the genome, which was once considered 'junk DNA,' actually has a role in regulating the activity of particular genes (gene expression).").

interests.' "[208] Importantly, our system of justice "do[es] not accept even [a] small level of intrusion, [such as fingerprinting] for free persons without Fourth Amendment constraint."[209]

Here, the government's interest in identification of criminals must be weighed against the interests of free individuals in maintaining control over their genetic privacy. While the government and society have a strong interest in identifying criminals—particularly violent criminals like serial killers and rapists—keeping them off the streets, and preventing crimes, this should not be permitted at the complete expense of individuals' genetic privacy without regulations or Fourth Amendment protection. While the Fourth Amendment requires that searches be reasonable, "what is reasonable depends on the context within which a search takes place."[210] Here, DNA's extremely revealing nature and its ability to implicate countless individuals tips the balance toward the interest of the individual in a way that fingerprinting simply does not.

B. The Anonymization of Genetic Information in Recreational Databases is Ineffective and Thus Insufficient to Protect Genetic Privacy

Some may argue that because recreational DNA companies anonymize the genetic information stored in their databases, individuals' genetic privacy is sufficiently protected. However, this solution is superficial and unrealistic. First, it is important to note that DNA submitted to recreational DNA websites often does not remain solely with those websites. In fact, many commercial genealogy companies ultimately plan to sell customers' genetic information to pharmaceutical companies or medical researchers, if they do not do so already.[211] Additionally, commercial sites have little control as to where this information may eventually end

---

[208] United States v. Davis, 690 F.3d 226, 247 (4th Cir. 2012) (quoting Samson v. California, 547 U.S. 843, 848 (2006)).

[209] *Id.* at 245 (quoting Jones v. Murray, 962 F.2d 302, 306 (4th Cir. 1992)).

[210] Maryland v. King, 569 U.S. 435, 461–62 (2013) (quoting New Jersey v. T.L.O., 469 U.S. 325, 337 (1985)).

[211] *See* Scutti, *What the Golden State Killer Case Means*, *supra* note 14. For example, GlaxoSmithKline recently reached a deal with 23andMe to acquire a $300 million stake in the genealogy company. Brodwin, *supra* note 93. GlaxoSmithKline plans to use 23andMe's data "to look for new drugs to develop . . . [and] inform how patients are selected for clinical trials." *Id.*; *see also infra* note 123 (Verogen Inc.'s purchase of GEDmatch). "We ask these sites to be responsible stewards of our information, but they are nevertheless subject to incentives to make millions by selling our data to others." Bala, *supra* note 25.

up.[212] Frighteningly, the inability to determine who possesses one's genetic information may mean that it could be extraordinarily difficult to prove that an employer or insurer is engaging in genetic discrimination and subject to the Genetic Information Nondiscrimination Act, if one even suspects such a possibility.[213]

Second, while commercial genealogy companies contend that any genetic information shared with the company is anonymized, true anonymization can neither be achieved nor guaranteed.[214] Benjamin Berkman, a National Institutes of Health bioethicist, stated that while companies can tout all the "procedural and technical safeguards . . . put in place to protect the confidentiality of [people's] data," anonymity can, nevertheless, not be promised.[215] This is because a person's anonymized DNA can be re-identified in a fairly simplistic way. In a recent study, for example, Yaniv Erlich's team found that "[o]nce relatives are found, an anonymous person can be re-identified by constructing a family tree, searching for additional relatives and then triangulating from there."[216] In this way, Erlich's team was able to "re-identif[y] a woman from her 'anonymous'—though publicly available—DNA information."[217]

Most concerning in the criminal context, however, is a recent study that found that DNA may be used to identify individuals and their relatives by cross-referencing the STR DNA in CODIS with the SNP DNA in recreational databases and vice versa.[218] This

---

[212] Scutti, *What the Golden State Killer Case Means*, *supra* note 14 ("When a company shares de-dentified [*sic*] and aggregated data with partners they [*sic*] cannot guarantee what will happen to the information once it leaves their hands."); Brodwin, *supra* note 93 ("[L]eaks can happen, and privacy advocates say that such incidents could allow your data to find its way elsewhere, perhaps without your knowledge.").

[213] Fox, *supra* note 164.

[214] Scutti, *What the Golden State Killer Case Means*, *supra* note 14 ("[W]hen it comes to 'anonymizing' DNA, it is so far impossible to truly do so . . . .").

[215] Stein, *supra* note 16.

[216] 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 [hereinafter Scutti, *You Might Not Be Anonymous*].

[217] *Id.* The team was able to successfully re-identify this woman "using her anonymized DNA profile and birth date, which is often publicly available to researchers." Kaiser, *supra* note 17. Notably, this was not the first time that attempts to re-identify "anonymous" DNA samples were successful. In 2013, researchers at the Whitehead Institute for Biomedical Research re-identified "[fifty] people from DNA donated anonymously for scientific study using easily available internet databases." Fox, *supra* note 164.

[218] *See* Jaehee Kim et al., *Statistical Detection of Relatives Typed with Disjoint Forensic and Biomedical Loci*, 175 CELL 848, 848 (2018).

discovery is significant in that it suggests the use of commercial and criminal DNA databases in ways "not intended in the context of either database examined in isolation."[219] Noah Rosenberg, one of the authors of the study, explained the significance simply, stating that "[d]ifferent databases constructed for different purposes might independently not provide enough information to reveal a person's identity but by combining information from multiple databases identifications can be made."[220] A recreational DNA profile linked to a profile in CODIS, for example, "could . . . reveal physical appearance or medical information for a criminal or their relatives, such as genes for eye color or a disease, even though the forensic databases aren't supposed to contain that kind of information."[221] Again, this raises a significant privacy concern not only for free individuals who may or may not have submitted their DNA to commercial companies but who are nevertheless included in such searches, but also for individuals who have come into contact with the criminal justice system and have DNA profiles in CODIS. This is yet another scenario where anonymization of genetic information in DNA databases falls short in protecting individuals' genetic privacy.

C. Despite the Time Consuming and Work-Intensive Nature of Familial Searching, Stringent Regulation Is Necessary

While it is unclear how often law enforcement conducts familial searches in recreational and commercial DNA databases,[222] some try to mitigate the concerns surrounding the technique by arguing that it will not be used frequently, as it requires a substantial amount of time and personpower.[223] The argument is that familial searching in recreational DNA databases has the potential to "generate an extraordinary number of leads, and running them all down using both nongenetic and genetic information requires a lot of police power."[224] The accuracy of this statement is demonstrated by the effort to identify Joseph James DeAngelo Jr. as the Golden State Killer, which entailed "a

---

[219] *Id.*

[220] Scutti, *You Might Not Be Anonymous*, *supra* note 216.

[221] Kaiser, *supra* note 17.

[222] Kolata & Murphy, *supra* note 1; Hesman Saey, *supra* note 8 ("[T]here's no telling how many people in . . . public database[s] are being subjected to what amounts to a 'genetic stop and frisk.' ").

[223] Hesman Saey, *supra* note 8; Kolata & Murphy, *supra* note 1 ("I doubt it will be run of the mill any time soon.").

[224] Kolata & Murphy, *supra* note 1.

team of five investigators [who] spent four months building out family trees, name by name. [The team] pored over census records, newspaper obituaries, gravesite locaters, and police and commercial databases to find each relative and, ultimately, DeAngelo."[225] Furthermore, others note that the concerns surrounding increased forensic use of recreational DNA databases are overstated.[226] An investigative genetic genealogist, for example, criticized recent studies that demonstrate the vast identification capabilities of DNA in recreational databases, and argued that the researchers "ma[d]e a lot of assumptions that aren't in line with reality, . . . [by] assuming some head-starts" not necessarily available to investigative genealogists.[227]

However, neither infrequent use of familial searching in recreational DNA databases nor inconsistent access of investigators to "critical demographic information"[228] present sufficient rationales for not protecting genetic information. The necessity of Fourth Amendment protection is not premised upon how much effort it would take law enforcement to access one's information, and the public need not place trust in law enforcement's voluntary decisions regarding whether or not to utilize familial searching in recreational DNA databases.[229] Furthermore, as genetic research and computer technology advance, it is not unforeseeable that less personpower would be required to utilize this technique in the future.[230] While it took investigators four months to identify the Golden State Killer, for example, it took the Sacramento District Attorney's office only ten days to identify the NorCal Rapist using the same techniques.[231] Because it is impossible to predict the extent of the information

---

[225] Jouvenal, *supra* note 2.

[226] Johnson, *supra* note 15.

[227] *Id.* ("[R]eal cases would often lack the critical demographic information—such as the age and family tree—that the academic researchers used in their sample case.").

[228] *Id.*

[229] *Cf.* Katz v. United States, 389 U.S. 347, 356–57, 358–59 (1967).

[230] "[M]atches will become more frequent" as more people submit their DNA samples to recreational DNA services. Molteni, *supra* note 12. Furthermore, researchers are currently working to develop and "perfect rapid DNA machines [that] can generate DNA profiles within hours," and it has been predicted that there may be "handheld DNA devices" within the next ten to twenty years. N'dea Yancey-Bragg, *DNA is Cracking Mysteries and Cold Cases. But is Genome Sleuthing the 'Unregulated Wild West?'*, USA TODAY (May 14, 2019), https://www.usatoday.com/story/news/nation/2019/05/14/heres-how-dna-cracking-cold-cases-and-exonerating-innocent/1159571001/.

[231] Molteni, *supra* note 12.

DNA may reveal, how this information may be used in the future and by whom, and because the personal information of countless individuals is implicated, statutory protections are necessary to protect the information in these databases.

IV. STATUTORY PROTECTIONS ARE REQUIRED TO SAFEGUARD GENETIC INFORMATION STORED IN RECREATIONAL DNA DATABASES

While law enforcement's use of familial searching in commercial and recreational DNA databases is just beginning, there are indications that this technique may become more prevalent in the future.[232] As the DNA stored in these databases will soon have the potential to identify nearly everyone, the privacy implications of forensic use of these databases are far-reaching.[233] Furthermore, law enforcement's unregulated access to the genetic information stored in these databases has the potential to result in unwarranted invasions of privacy, whether or not people volunteered their own DNA samples. "A person's privacy in the contents of each microscopic bundle of DNA should be more stringently protected because of the unpredictability and density of the genetic information it contains."[234] Without statutory protections, society must place its trust that genetic privacy will be respected and protected in the hands of companies that profit by exploiting this information. Most unrealistically, these companies would have to voluntarily agree on how DNA information should be protected.[235] It is thus imperative that statutory protections be implemented to safeguard individuals' genetic privacy.

Some statutory suggestions consider ways in which the genetic information itself may be protected. For example, Yaniv Erlich recommends "that all genetic information be encrypted to

---

[232] *See* Zhang, *The Coming Wave of Murders Solved*, *supra* note 12 (highlighting one hundred crime scene DNA samples recently uploaded to GEDmatch); *see also supra* note 119 and associated text.

[233] Kaiser, *supra* note 17; *see also* Yancey-Bragg, *supra* note 230 ("It happens almost every week: Police reveal that DNA technology has helped them crack a decades-old case or identify an infamous serial killer like Jack the Ripper.").

[234] Lowenberg, *supra* note 15, at 1311.

[235] Kaiser, *supra* note 17 ("[A]ll the players in the direct-to-consumer DNA sequencing industry would have to agree to [a] scheme . . . . 'If not, we're back to square one.' " (quoting Natalie Ram, a law professor at the University of Baltimore in Maryland)).

protect the information."[236] However, this suggestion alone is insufficient to protect genetic information and prevent DNA from being re-identified. Even if a commercial genealogy company were to be required to encrypt the data submitted to it, this would not protect the genetic information already shared with medical researchers and pharmaceutical companies. Furthermore, to maintain protection, every time the information was shared or sold, the information would have to be decrypted and the following party would then have to re-encrypt it. Any statutory protection that includes encryption would have to require such a process.

Other suggested statutory protections focus on the importance of informed consent and ensuring that people are aware of the possibility that their genetic information may be used in criminal investigations. Denise Syndercombe Court, a professor in the Forensic Science Research Group at King's College London, suggests that companies openly provide "information about both the benefits and risks to individuals," instead of hiding this information in the terms of service.[237] Erin Murphy, a professor of law at New York University, goes a step further, adding that "compulsory disclosure of law enforcement activity" should be required.[238] While requiring such communication would be a step in the right direction with regard to individuals who submit their DNA directly to commercial genealogy companies, this solution does not address genetically related individuals' lack of opportunity to provide informed consent.[239]

Some have suggested banning familial searches in recreational DNA databases altogether.[240] This suggestion may be too extreme, however, as it does not take into consideration the significant societal interest in solving past crimes and preventing future crimes, nor does it recognize that this tool may be useful if used properly. A more realistic solution is one that would focus on limiting how and when familial searching in recreational DNA databases may be used. A common suggestion is that the use of this technique be used sparingly, only to solve violent crimes like rape and murder,[241] or only "when all other investigative

---

[236] Stein, *supra* note 16.

[237] Syndercombe Court, *supra* note 171, at 203.

[238] Murphy, *supra* note 36, at e8.

[239] *See supra* Section II.A.4.

[240] *See*, *e.g.*, Murphy, *supra* note 36, at e8.

[241] *See* Rainey, *supra* note 183; *see also* Kaiser, *supra* note 17 ("It may be reasonable for a murder case, but not for a petty crime . . . . 'Finding the right balance is important.' ").

approaches have failed."[242] While there are significant differences in the STR DNA in CODIS and the SNP DNA in recreational databases, an important first step in regulating the use of familial searching in recreational databases would be to impose similar protections on the recreational databases as exist to regulate CODIS.[243]

CONCLUSION

While familial searching in recreational DNA databases may be an effective new tool for law enforcement, there currently exists a serious lack of protection for the genetic privacy of those who submitted DNA samples, and those to whom they are genetically related. Like the CSLI information discussed in *Carpenter v. United States*, DNA information is profoundly revealing, illustrating a person's fundamental personhood.[244] DNA also has the unique ability to reveal who a person is related to, implicating countless others, past, present, and future.[245] Again, as the Supreme Court proclaimed in *Carpenter*, "as '[s]ubtler and more far-reaching means of invading privacy have become available to the Government' [we must] ensure that the 'progress of science' does not erode Fourth Amendment protections."[246] It remains to be seen whether the Supreme Court will deem DNA a unique type of data and whether it will find familial searching in recreational databases subject to Fourth Amendment protections. In the meantime, the implementation of statutory protections is crucial to regulate whose DNA data may be accessed or used, by whom, how, and under what circumstances. As Erin Murphy eloquently stated, "[b]ig genome data has arrived; it is time to do something more than gape in wonder at it."[247]

---

[242] Rainey, *supra* note 183.

[243] Murphy, *supra* note 36, at e8.

[244] *See supra* Section I.B.

[245] *See supra* Section I.A.

[246] Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (quoting Olmstead v. United States, 277 U.S. 438, 473–74 (1928) (Brandeis, J., dissenting)).

[247] Murphy, *supra* note 36, at e8.