COURTS & JUSTICE LAW JOURNAL

GENETIC STANDING: THE CONSTITUTIONALITY OF FAMILIAL DNA SEARCHING ON GENEALOGICAL RESEARCH DATABASES

*Emily M. Strak**

INTRODUCTION

In *Carpenter v. United States*, the United States Supreme Court recognized that the nation's cell phone service accounts exceed its population.[1] Comparably, the consumer market for genetic testing is climbing rapidly.[2] In 2017, the most popular direct-to-consumer[3] genetic testing company, Ancestry.com, completed genetic testing on four million

* Emily Strak is a rising 3L at Regent University School of Law. I would like to thank my faculty advisor, James Duane, for his expert guidance throughout the writing process. I would also like to thank my husband, Mark, and my two young sons, Mason and Matthew, who encourage me each and every day.

[1] 138 S. Ct. 2206, 2211 (2018) ("There are 396 million cell phone service accounts in the United States—for a Nation of 326 million people.")

[2] Heather Murphy, *Most White Americans' DNA can be Identified Through Genealogy Databases*, N.Y. TIMES (Oct. 11, 2018), https://www.nytimes.com/2018/10/11/science/science-genetic-genealogy-study.html [hereinafter Murphy, *Genealogy Databases*].

[3] Direct-to-consumer, also known as direct selling, is where manufacturers or producers bypass a wholesaler and sell directly to the consumer. *Direct Selling*, MERRIAM-WEBSTER.COM, https://www.merriam-webster.com/dictionary/direct%20selling (last visited Feb. 9, 2019).

people.[4] The second most popular company, 23andMe, held a spot on Amazon's list of top sellers on Black Friday Weekend for 2017.[5] Whether seeking ancestral origins, uncovering genetic health risks, or determining the likelihood of growing a unibrow, more than fifteen million consumers have submitted some form of their deoxyribonucleic acid (DNA) to a direct-to-consumer genetic testing company.[6] Upon receiving their results, consumers then may download their "lab-generated information of a DNA sample," also called raw DNA data.[7] Once downloaded, consumers may upload their raw DNA data to a third-party website to conduct independent genealogy and ancestry research.[8]

Currently, the most popular website used for this research is GEDmatch.com.[9] GEDmatch shares DNA information by revealing partial DNA matches between its members.[10] It is a useful genealogy research tool because GEDmatch does not limit the type of DNA data it will accept as long as the user uploads the data in an approved format.[11] In 2018, law enforcement agencies began using GEDmatch as an investigative tool to solve cold cases through familial DNA searching.[12] Familial DNA searching intentionally looks for a partial DNA match instead of an exact

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

[5] *Id.*

[6] Murphy, *Genealogy Databases*, *supra* note 2; 23ANDME, https://www.23andme.com/dna-health-ancestry/(last visited Oct. 14, 2018).

[7] *Downloading Raw DNA Data*, ANCESTRY.COM, https://support.ancestry.com/s/article/Downloading-Raw-DNA-Data-1460089696533 (last visited Nov. 18, 2018).

[8] Susan Scutti, *You Might Not be Anonymous, Thanks to Genealogy Databases*, CNN.COM, (Oct. 11, 2018, 3:47 PM), https://www.cnn.com/2018/10/11/health/genetic-privacy-study/index.html.

[9] GEDMATCH, https://www.gedmatch.com/tos.htm (last visited Oct. 22, 2018). While there are other third-party websites that allow users to upload their raw DNA data for genealogical-based research, this article primarily focuses on GEDmatch.

[10] *Id.*

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

[12] *Id*.

match.[13] By utilizing in-house forensic specialists or by hiring independent genealogists, investigators can upload raw data from preserved crime scene DNA and search GEDmatch's database for a partial match.[14] If GEDmatch reveals a partial match, expert genealogists can take that match and build a family tree.[15] With enough time and resources, the family tree construction has successfully led law enforcement to a suspect.[16] A subsequent DNA analysis between the suspect's DNA and the preserved crime scene DNA will confirm whether the police have in fact found the correct person.[17]

This article examines the potential constitutional issues raised when law enforcement agencies conduct familial DNA searching on genealogical research databases, such as GEDmatch. Part I of this article provides basic information on forensic DNA testing, such as the differences between forensic DNA testing and genetic DNA testing. Part II provides a basic description of familial DNA searching and describes how law enforcement agencies nationwide are using GEDmatch as a familial DNA searching tool. Part III provides historical background and development on Fourth Amendment analysis and case law. Part IV attempts to determine whether familial searching conducted by law enforcement agencies on GEDmatch is a search under the Fourth Amendment.[18] Additionally, if familial searching on genealogical research databases, such as GEDmatch, is a search under the Fourth Amendment, Part IV also tries to uncover who would have standing to assert a Fourth Amendment violation.[19] Part V addresses the exceptions to the Fourth Amendment search doctrine that are

[13] Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291, 297–98 (2010) [hereinafter Murphy, *Relative Doubt*].

[14] Crimesider Staff, *Privacy Concerns After Public Genealogy Database Used to ID "Golden State Killer" Suspect*, CBS NEWS (Apr. 27, 2018, 6:48 PM), https://www.cbsnews.com/news/privacy-concerns-after-public-genealogy-database-used-to-id-golden-state-killer-suspect/ [hereinafter Crimesider Staff, *Privacy Concerns*].

[15] *Id.*

[16] *Id.*; *see also* Murphy, *Relative Doubt*, *supra* note 13, at 298 (stating that if the database contains a relative to the DNA sample, a large enough search threshold is 80–90% likely to populate that relative as a partial match).

[17] Crimesider Staff, *Privacy Concerns*, *supra* note 14.

[18] *See* discussions on Fourth Amendment search analysis using the "reasonable expectation of privacy" standard and the traditional "property intrusion" standard *infra* Part IV, Sections 1 & 2, respectively.

[19] *See* discussion on constitutional standing *infra* Part IV, Section 3.

applicable to law enforcement's use of GEDmatch. And finally, Part VI proposes that, at least for the immediate future, the best approach to regulate law enforcement's use of GEDmatch is through statutory regulation.

I. FORENSIC DNA TYPING VS. GENEALOGICAL RESEARCH DNA TYPING

A person's genetic information is coded within his DNA by using a series of four chemical bases: adenine, guanine, cytosine, and thymine, (abbreviated as A, G, C, and T).[20] Human DNA contains a total of roughly three billion bases, of which over 99% are identical in every human.[21] Because DNA is inherited in established patterns, genetic information is not absolutely unique to each individual.[22] For instance, a father passes down the Y chromosome, present only in males, to each of his sons.[23] As a result, the Y chromosome within a DNA profile may recognize a particular paternal line, but its presence is not unique to one individual male.[24] Likewise, only a mother can pass down mitochondrial DNA; therefore, descendants of the same mother share the same or nearly identical mitochondrial DNA sequence.[25] Accordingly, a mitochondrial DNA sequence cannot identify individuals but it may identify families.[26]

However, everyone's DNA is distinguishable by looking at differences in patterns within particular DNA strands, called "microsatellites."[27] "Single-tandem repeat" (STR) is the most common forensic DNA typing used by law enforcement agencies in the United States.[28] STR examines thirteen different genomic locations ("loci") on the microsatellites, which present "two variants of repeat lengths, one pattern

[20] U.S. Nat'l Library of Med., *What is DNA?*, GENETICS HOME REFERENCE, https://ghr.nlm.nih.gov/primer/basics/dna (last visited Oct. 23, 2018).

[21] *Id.*

[22] Natalie Ram, *DNA by the Entirety*, 115 COLUM. L. REV. 873, 878 (2015).

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] Murphy, *Relative Doubt*, *supra* note 13 at 295.

[28] *Id.*; *STR Analysis*, NAT'L INST. OF JUST., https://www.nij.gov/journals/267/pages/extending-str.aspx (last visited Dec. 10, 2018).

inherited from each genetic parent."[29] In total, twenty-six data points are examined and this analysis is what makes up a person's forensic genetic profile.[30] STRs are also known as "junk" genes because the strands contain minimal, if any, medical information about an individual—their *only* purpose is for identification.[31]

In contrast, most genealogical research and direct-to-consumer genetic testing companies use a DNA typing called single nucleotide polymorphisms (SNP).[32] SNP typing looks for maternal and paternal inherited variations within an individual's DNA sequence.[33] Unlike STR strands, which have little genetic value beyond identification, SNP strands contain valuable genetic information, such as an individual's disease carrier status.[34] Due to privacy concerns, law enforcement agencies generally do not use SNP typing within the criminal investigation context.[35]

Even the U.S. Supreme Court has discussed the privacy safeguards in using STR typing in the criminal justice context. For example, in *Maryland v. King*, the U.S. Supreme Court held that after an individual's arrest for a serious offense, obtaining his DNA through a buccal swab and analyzing his DNA for identification purposes was reasonable under the Fourth Amendment.[36] Maryland police arrested King and charged him with

[29] Ram, *supra* note 22, at 880–81.

[30] *Id.* at 881.

[31] Erin Murphy, *Law and Policy Oversight of Familial Searches in Recreational Genealogy Databases*, FORENSIC SCI. INT'L 292, e5 (Aug. 31, 2018) https://doi.org/10.1016/j.forsciint.2018.08.027 [hereinafter Murphy, *Policy Oversight*].

[32] *Id.*

[33] *Id.*

[34] *Id.* For example, through SNP typing, 23andMe offers its consumers over five "Genetic Health Risk Reports" that reveal an individual's "genetic risk based on a limited set of variants for breast, ovarian and other cancers," an individual's "genetic risk for a form of adult-onset vision loss," and an individual's "genetic risk for lung and liver disease." *DNA Reports List*, 23ANDME.COM, https://www.23andme.com/dna-reports-list/ (last visited Feb. 9, 2019).

[35] *Id.* at e5–e6. (stating that in rare cases, law enforcement agencies have used SNP typing to distinguish the identities of twins).

[36] Maryland v. King, 569 U.S. 435, 465–66 (2013); *Id.* at 444 (A "buccal swab" is a cell collection process where a cotton swab is rubbed on the inside of an individual's cheek to collect skin cells.).

first and second-degree assault.[37] Police obtained King's DNA through a buccal swab, a standard booking procedure for any suspect charged with a serious offense.[38] The DNA analysis revealed that King's DNA matched an unidentified DNA sample retrieved from a rape victim several years earlier.[39] Maryland ultimately charged and convicted King for the rape.[40] The Court justified the DNA analysis because "the [STR] loci come from noncoding parts of the DNA that do not reveal genetic traits of the arrestee."[41] The Court agreed that while STR typing did not reveal information beyond identification, further advances in DNA typing may have Fourth Amendment violations.[42]

II. FAMILIAL DNA SEARCHING

During a routine search, when both the DNA sample and a DNA profile within the searched database share several of the same loci, it is known as a "partial match."[43] Unlike partial matches, which are coincidental, familial searching on a particular DNA database is a deliberate, intentional search for a biological relative versus searching for an exact match of the DNA sample.[44] Because law enforcement agencies use STR typing, the results of familial DNA searching on a government DNA database, such as the National DNA Index System (NDIS), are limited to the individual's immediate family.[45] However, the results of familial searching on GEDmatch, which contain SNP profiles, typically include much more of the sample's extended family.[46] This is again due to the vast amount of information contained within an SNP strand.[47] If a relative is

[37] *Id.* at 440–41.
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] *Id.* at 464.
[42] *Id.*
[43] *Frequently Asked Questions on CODIS and NDIS*, FBI.GOV, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet (last visited Dec. 5, 2018) [hereinafter FBI, *Questions*].
[44] *Id.*
[45] Murphy, *Policy Oversight*, *supra* note 31, at e6.
[46] *Id.*
[47] *Id.* at e5.

found through familial DNA searching, investigators may identify the preserved crime scene DNA sample through a "triangulation of data," which involves constructing a family tree, searching for more relatives through other public DNA forums, and utilizing other collection methods.[48]

At this time, federal law enforcement agencies are not authorized to perform familial DNA searching within the NDIS.[49] At the state level, each state determines whether and to what extent its law enforcement agencies are authorized to perform familial DNA searches.[50] Specifically, in Virginia "[t]he Virginia Department of Forensic Science has been permitted to conduct a limited number of . . . familial DNA searches of state and federal DNA databases since 2012."[51] As of April 2018, the department states it has not performed a search using a private genealogical website.[52]

While familial DNA searching has been employed as an investigative tool since 2002, it was not until early 2018 that law enforcement successfully made its first arrest from using a familial search on GEDmatch.[53] In April 2018, police arrested Joseph James DeAngelo, more commonly known as the "Golden State Killer," after police hired experts who traced his family tree using GEDmatch for four months.[54]

---

[48] Scutti, *supra* note 8.

[49] *Id.*

[50] *Id.* Currently, Arkansas, California, Colorado, Florida, Michigan, Texas, Utah, Virginia, Wisconsin, and Wyoming perform familial DNA searches on state-government DNA databases. Maryland and the District of Columbia passed statutes specifically prohibiting familial DNA searching. MD. CODE ANN., PUB. SAFETY § 2-506 (LEXIS through 2018 Reg. Sess.); D.C. CODE ANN. § 22-4151(West, Westlaw through Nov. 11, 2018).

[51] Frank Green, *DNA Search on a Genealogical Site not done in Virginia, but Raises Concerns*, ROANOKE TIMES (Apr. 27, 2018), https://www.roanoke.com/news/virginia/dna-search-on-a-genealogical-site-not-done-in-virginia/article_caf8984f-79e1-5a60-a201-4a288f7f2cad.html.

[52] *Id.*

[53] *See* Murphy, *Relative Doubt*, *supra* note 13, at 301 (stating that investigators working on a 1970s serial rape case conducted the first successful familial database search in 2002); Eric Levenson, *It Started as a Hobby. Now They're Using DNA to Help Cops Crack Cold Cases*, CNN.COM (Aug. 3, 2018, 3:19 PM), https://www.cnn.com/2018/08/03/health/dna-genealogy-cold-cases-trnd/index.html.

[54] Justin Jouvenal, *To Find Alleged Golden State Killer, Investigators First Found his Great-Great-Great-Grandparents*, THE WASH. POST (April 30, 2018),

Investigators discovered that the preserved crime scene DNA contained a rare Y chromosome genetic marker.[55] When police ran the preserved DNA through GEDmatch's database, it first led to a man in Oregon who had the same genetic marker.[56] After ruling out the Oregon man as a suspect, investigators went back to GEDmatch to analyze other partial DNA matches, including a distant cousin.[57] From that one familial match to the distant cousin, investigators determined that approximately 200 years ago, the suspect and his cousin shared a male relative.[58] By tracing the cousin's family tree, investigators were able to confine a list of suspects to "males born between 1940–1960, of the right physical size, who had resided in California during the years of the crimes."[59] Officers were eventually able to hone in on DeAngelo, and when police collected abandoned DNA from DeAngelo's trash and analyzed it against the crime scene DNA, it matched exactly.[60]

Since the arrest of DeAngelo, police have made at least fourteen more arrests by accessing and utilizing raw DNA data posted on GEDmatch by its members.[61] For example, police in Lancaster, Pennsylvania arrested Raymond Rowe in 2018 for the 1992 murder of Christy Mirack.[62] Police analyzed preserved semen from the 1992 crime scene and uploaded that DNA profile onto GEDmatch, where it partially matched with a DNA

---

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?utm_term=.e268da7b04d7; Jennifer Bucholtz, *Identifying the Golden State Killer*, In Public Safety (May 31, 2018), https://inpublicsafety.com/2018/05/identifying-golden-state-killer-investigator-details-role-ancestry-site/.

[55] Bucholtz, *supra* note 54.

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] *Id.*

[60] *Id.*; *see also* discussion on abandoned DNA *infra*, Part V, Section 1.

[61] Murphy, *Family History Website*, *supra* note 11.

[62] Maya Eliahou & Justin Lear, *A Piece of Chewing Gum, a Bottle of Water and New DNA Technology May Have Just Solved a Teacher's Murder*, CNN.COM (June 26, 2018, 7:33 PM), https://www.cnn.com/2018/06/26/us/christy-mirack-slaying-update-trnd/index.html. [hereinafter Eliahou, *New DNA Technology*].

profile of Rowe's relative.[63] The police analyzed Rowe's DNA, collected from a used water bottle and a chewed piece of gum, against the crime scene DNA.[64] The likelihood that the crime scene DNA belonged to anyone *but* Rowe was "approximately one in 200 octillions from the Caucasian population."[65]

Likewise, police arrested William Earl Talbott II in 2018, for the 1987 murders of Tanya Van Cuylenborg and Jay Cook.[66] Investigators hired a Virginia-based company, Parabon Nano Labs, which conducted genetic genealogy analysis.[67] Parabon uploaded DNA data derived from the crime scene to GEDmatch, and a familial search matched Talbott's distant cousin.[68] Similar to the Golden State Killer, a family tree traced from the cousin eventually pointed to Talbott.[69] Police analyzed Talbott's abandoned DNA to confirm that his DNA matched the DNA from the crime scene.[70]

GEDmatch has never aligned itself as a law enforcement investigative tool. On its website, GEDmatch states that its purpose is:

> to provide DNA and genealogy tools for comparison and research purposes. It is supported entirely by users, volunteers, and researchers. DNA and Genealogical research, by its very nature, requires the sharing of information. Because of that, users participating in this Site agree that their information will be shared with other users.[71]

---

[63] *Id.*

[64] *Id.*; *see also* discussion on abandoned DNA *infra*, Part V, Section 1.

[65] Eliahou, *New DNA Technology*, *supra* note 62.

[66] Crimesider Staff, *Suspect Linked to Couple's 1987 Killing Through Public Genealogy Site Charges with Murder*, CBS NEWS, (June 19, 2018, 7:17 PM), https://www.cbsnews.com/news/suspect-linked-to-couples-1987-killing-with-public-genealogy-site-charged-with-murder/ [hereinafter Crimesider Staff, *Suspect*].

[67] *Id.*

[68] *Id.*

[69] *Id.*

[70] *Id.*; *see also* discussion on abandoned DNA *infra*, Part V, Section 1.

[71] GEDMATCH, *supra* note 9.

However, in spite of this statement, GEDmatch updated its terms of service and privacy statement since the news of DeAngelo's arrest went public.[72] As part of its updated terms of service and privacy statement, GEDmatch now allows law enforcement to upload raw DNA data so long as the "DNA obtained and authorized by law enforcement either: (1) identify a perpetrator of a violent crime against another individual; or (2) identify remains of a deceased individual."[73] GEDmatch defines violent crime "as homicide or sexual assault."[74] Overall, the general public favors using GEDmatch for identifying perpetrators of violent crimes. A recent study revealed that 80% of the participants surveyed supported law enforcement's use of private genetic websites, such as GEDmatch, when identifying perpetrators of violent crimes.[75] On the other hand, if law enforcement used private genetic websites as a tool to identify perpetrators of non-violent crimes, that support substantially dropped to only 39%.[76]

Unlike companies such as Ancestry.com or 23andMe, which will not release DNA data to law enforcement without a valid subpoena or warrant, GEDmatch's website allows anyone, including law enforcement, to create an account, upload raw DNA data and run that data against its database of other GEDmatch users.[77] While GEDmatch acknowledges that:

---

[72] *Id.* (stating that GEDmatch revised its terms of service and privacy statement on May 20, 2018); *see also supra* note 54 and accompanying text.

[73] GEDMATCH, *supra* note 9.

[74] *Id.*

[75] Christi J. Guerrini, *Should Police Have Access to Genetic Genealogy Databases? Capturing the Golden State Killer and Other Criminals Using a Controversial New Forensic Technique*, 16 PLOS BIOLOGY (2018), https://journals.plos.org/plosbiology/article?id=10.1371/journal.pbio.2006906#pbio.2006906.ref016.

[76] *Id.*

[77] *Compare Ancestry 2017 Transparency Report*, ANCESTRY.COM, https://www.ancestry.com/cs/transparency (last visited Dec. 6, 2018) (requiring "valid legal process in order to produces information about [its] members"), *and Transparency Report*, 23ANDME.COM, https://www.23andme.com/transparency-report/ (last visited Dec. 6, 2018) (stating that 23andMe uses "all practical legal and administrative resources" to resist government subpoenas, warrants, or order for its members information), *with GEDmatch.com Terms of Service and Privacy Policy*, GEDMATCH.COM, https://www.gedmatch.com/tos.htm (last visited Dec. 6, 2018) (stating that law enforcement may upload DNA information to "identify a perpetrator of a violent crime against another").

> [T]he results presented on this Site are intended *solely* for genealogical research, we are unable to guarantee that users will not find other uses, including both current and new genealogical and non-genealogical uses. For example, some of these possible uses of Raw Data, personal information and/or Genealogy Data by any registered user of GEDmatch include . . . [f]amilial searching by third parties such as law enforcement agencies to identify the perpetrator of a crime, or to identify remains.[78]

When a user uploads his raw DNA data to GEDmatch, he has the choice to classify the data one of three ways: as private, as public, or as research.[79] According to GEDmatch's terms of service, " 'Private' DNA data is not available for comparison with other people. It may be usable in some utilities that do not depend on comparisons with other DNA."[80] Alternatively, " 'Public' DNA is available for comparison to any Raw Data in the GEDmatch database . . . . Comparison results, including your kit number, name (or alias), and email will be displayed for anyone that shares DNA with a Raw Data profile . . . ."[81] Lastly, " 'Research' DNA data is available for one-to-one comparison to other Public or Research DNA."[82]

Currently, there are over seventeen million DNA profiles in GEDmatch's database.[83] A new study estimated that 60% of Americans with European descent are currently identifiable through familial DNA searching, either on GEDmatch or on another genealogical research database.[84] This same study also predicted that within the next three years, almost 100% of all Americans with European descent will be identifiable through this same process, even if they never posted their own DNA

[78] GEDMATCH, *supra* note 9 (emphasis added).
[79] *Id.*
[80] *Id.*
[81] *Id.*
[82] *Id.*
[83] Murphy, *Family History Website*, *supra* note 11.
[84] Y. Erlich et al., *Identify Inference of Genomic Data Using Long-Range Familial Searches*, SCIENCE MAG. 1 (2018), http://science.sciencemag.org/content/early/2018/10/10/science.aau4832/tab-pdf.

profile.[85] This means, an individual's decision to use GEDmatch or another genealogical research database not only discloses his own personal DNA information but it also reveals the DNA information of his biological family members.[86] Although a user's complete DNA Profile is not made fully public and the information is only revealed when there is a partial match of two DNA profiles, the seemingly unregulated use of GEDmatch puts a plethora of DNA information right at law enforcement's fingertips.[87] Furthermore, because NDIS and other government databases use STR typing and keep DNA within certain categories, generally prescribed by statute, GEDmatch arguably provides law enforcement officials access to DNA profiles and information that they would otherwise not have access to.[88]

III. THE HISTORY OF THE FOURTH AMENDMENT

The Fourth Amendment of the United States Constitution protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . ."[89] "The basic purpose of this Amendment. . . is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."[90] The Founding Fathers drafted the Fourth Amendment as a reaction to the colonial era "general warrants" and "writs of assistance," which gave British officers authority to search a person's home without any probable cause.[91]

Because the Fourth Amendment's language includes "houses, papers, and effects," a close relationship to real and personal property linked the Fourth Amendment search doctrine to common-law trespass for much of the country's history.[92] Described by the Supreme Court as a "true and

[85] *Id.*

[86] Bucholtz, *supra* note 54.

[87] Murphy, *Policy Oversight*, *supra* note 31, at e6.

[88] 34 U.S.C.A. § 12592 (Westlaw through P.L. 115-231); FBI, *Questions, supra* note 43.

[89] U.S. CONST. AMEND. IV.

[90] Camara v. Mun. Ct. of S.F., 387 U.S. 523, 528 (1967).

[91] Riley v. California, 134 S. Ct. 2473, 2494 (2014).

[92] *See* United States v. Jones, 565 U.S. 400, 405 (2012) (stating that without that close connection, "the phrase 'in their persons, houses, papers, and effects' would have been

ultimate expression of constitutional law," and as "sufficiently explanatory of what was meant by unreasonable searches and seizures," the English case, *Entick v. Carrington*, stated:

> [O]ur law holds the property of every man so sacred, that no man can set his foot upon his neighbour's close without his leave; if he does he is a trespasser, though he does no damage at all; if he will tread up his neighbour's ground, he must justify it by law.[93]

Until the mid-twentieth century, the Supreme Court held that a search violated the Fourth Amendment only when it was an *actual physical invasion* upon the person's tangible property.[94]

In 1967, the Supreme Court changed its position in *Katz v. United States*, when it stated that "the Fourth Amendment protects people, not places."[95] What had been previously considered a lawful search because it lacked the characteristics of a physical property invasion was now considered unlawful because, as the Court stated, "what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[96] The Court realized that technology, specifically the telephone, now made it possible to intrude into a person's personal life without invading his physical property.[97] In his concurring opinion, Justice Harlan described a two-fold approach that the Supreme Court later adopted and what is known today as the "reasonable expectation of privacy" standard.[98]

---

superfluous").

[93] Boyd v. United States, 116 U.S. 616, 626–27 (1886); 95 Eng. Rep. 807 (C. P. 1765).

[94] *See* Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding that wiretapping was not a search under the Fourth Amendment because "one who installs . . . a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wire beyond his house")

[95] 389 U.S. 347, 351 (1967).

[96] *Id.*; *Compare* Olmstead, 277 U.S. at 466 (stating the wiretapping did not amount to a search under the Fourth Amendment), *with* Katz, 389 U.S. at 351 (stating that "[t]he Government's activities in electronically listening to and recording the petitioner's words . . . constituted a 'search and seizure' within the meaning of the Fourth Amendment").

[97] Katz, 389 U.S. at 352–53.

[98] Katz, 389 U.S. at 361 (Harlan, J., concurring); *see also* Smith v. Maryland, 442 U.S. 735,740 (stating that Fourth Amendment protection must be a "'legitimate expectation of

He stated a person must first have exhibited a subjective "actual expectation of privacy" and second, that the expectation must be one that society recognizes as "reasonable."[99]

There has been some divisiveness on whether the holding in *Katz* effectively rejected the earlier property-based approach.[100] Before the Supreme Court's 2012 decision in *United States v. Jones*, the consensus among legal scholars was that it had.[101] However, the majority opinion in *Jones* emphasized that *Katz* neither eliminated nor narrowed the scope of the property rights component to the Fourth Amendment; rather, the Court stated:

> We have embodied that preservation of past right in our very definition of "reasonable expectation of privacy" which we have said to be an expectation "that has a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." [102]

As Justice Scalia stated in his majority opinion in *Kyllo v. United States*, "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[103] In a span of fewer than 100 years, the Supreme Court has tackled Fourth Amendment issues on wiretapping private and public telephones, GPS trackers, infrared surveillance and most recently cell phone data.[104] As technology continues to advance, the Supreme Court

---

privacy' that has been invaded by government action").

[99] Katz, 389 U.S. at 361 (Harlan, J., concurring).

[100] *See* Orin S. Kerr, *The Fourth Amendment and New Technologies*, 102 MICH. L. REV. 801, 817 (2004) (stating existing legal scholarship in the early 2000s teaches that "*Katz* rejected the property-based view [in *Olmstead*] and replaced it with a 'reasonable expectation of privacy' ").

[101] 565 U.S. 400, 409 (2012) (stating that "the Katz reasonable-expectation-of-privacy test has been *added* to, not *substituted for*, the common-law trespassory test"); Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 572 (2017).

[102] Jones, 565 U.S. at 407–08 (quoting Minnesota v. Carter, 525 U.S. 83, 88 (1998)).

[103] 533 U.S. 27, 33–34 (2001).

[104] *See, e.g.*, Carpenter, 138 S. Ct. 2206, 2220 (2018) (holding that the Government

will inevitably have to make even more difficult decisions on what is considered a search under the Fourth Amendment. The next section, Part IV, attempts to answer whether the government's use of GEDmatch and other genealogical databases constitutes a search under the Fourth Amendment. Section 1 analyzes this question under Justice Harlan's "reasonable expectation of privacy" standard, and Section 2 analyzes the same question under the traditional property intrusion standard resurrected in *Jones*.[105] Finally, Section 3 addresses issues regarding constitutional standing.[106]

IV. ARE FAMILIAL DNA SEARCHES PERFORMED ON GENEALOGICAL DATABASES SEARCHES UNDER THE FOURTH AMENDMENT?

A. *Reasonable Expectation of Privacy*

In the Supreme Court's recent decision in *Carpenter v. United States*, the Court acknowledged the historical importance of understanding what was considered "an unreasonable search and seizure when [the Fourth Amendment] was adopted."[107] On this understanding, the Supreme Court adheres to some basic principles regarding the Fourth Amendment—that it "seeks to secure 'the privacies of life' against 'arbitrary power,' " and "that a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.' "[108] On several occasions, advancing

obtaining cell-site location information (CSLI) is a search under the Fourth Amendment); Riley v. California, 134 S. Ct. 2473, 2494 (2014) (holding that "the search incident to arrest exception does not apply to cell phones"); Maryland v. King, 569 U.S. 435, 462 (2013) (holding that "[a] brief intrusion of an arrestee's person is subject to the Fourth Amendment" but a cheek buccal swab to obtain a DNA sample "does not increase the indignity already attendant to normal incidents of arrest"); Jones, 565 U.S. at 404 (holding "that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a "search"); Kyllo, 533 U.S. at 34–35 (holding that "information obtained by the thermal imager in this case was the product of a search"); *see also* cases cited *supra* note 96.

[105] *See supra* notes 98–102 and accompanying text.

[106] *See* discussion *infra* Part IV, Section 3.

[107] Carpenter, 138 S. Ct. at 2214 (quoting Carroll v. United States, 267 U.S. 132, 149 (1925) (internal quotation marks removed).

[108] *Id.* (first quoting Boyd v. United States, 116 U.S. 616, 630 (1886); then quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

technology has prompted the Supreme Court to reject a "mechanical interpretation" of the Fourth Amendment to preserve the same level of privacy from the government that existed at the Fourth Amendment's creation.[109] "[T]he 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."[110] Without these principles guiding the Supreme Court's decisions, law enforcement officials could exploit technological advances and circumvent the Fourth Amendment.[111]

Regarding internet activity, the Court stated in *Carpenter* that "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere."[112] In today's technologically advanced world, the "public sphere" may be easily defined as the internet or as a public street.[113] Just because most Americans conduct several components of their lives on the internet does not necessarily mean that they must relinquish all reasonable expectations of privacy.[114] So long as a subjective "actual expectation of privacy" that society recognizes as "reasonable" exists, Fourth Amendment protections should apply.[115]

Conversely, while a few lower courts have defined DNA analysis as a separate search under the Fourth Amendment, the Supreme Court's focus on Fourth Amendment searches remains on how the government *obtains* the data and not how the government *uses* the data.[116] For example, the Ninth Circuit acknowledged in *Rise v. Oregon* that "DNA genetic pattern

[109] *Id.*

[110] *Id.* at 2223 (quoting Olmstead v. United States, 277 U.S. 438, 473–74 (1928) (Brandeis, J., dissenting).

[111] *See* Kyllo, 533 U.S. 27, 35 (2001) (stating that a mechanical interpretation of the Fourth Amendment would "leave the homeowner at the mercy of advancing technology").

[112] Carpenter, 138 S. Ct. at 2217.

[113] *See* United States v. Irving, No. 18-10019, 2018 U.S. LEXIS 167088, at *7 (D. Kan. Sep. 28, 2018) ("The fact that the majority of an individual's information may be found on a 'public' portion of Facebook does not mean that one gives up any expectation of privacy.")

[114] Green, *supra* note 51.

[115] *See supra* note 98–103 and accompanying text.

[116] Ric Simmons, *The Mirage of Use Restrictions*, 96 N.C. L. REV. 133, 136 (2017).

analysis is even *more intrusive* than the blood alcohol test . . . ."[117] Likewise, in 2012 the Fourth Circuit held in *United States v. Davis* that DNA analysis was a search because a person retains a "legitimate expectation of privacy" in the information obtained from that analysis.[118] However, the Supreme Court declined to adopt this approach just a year later in *Maryland v. King* when it held that the subsequent "analysis of respondent's DNA pursuant to CODIS [Combined DNA Index System] procedures did not amount to a significant invasion of privacy that would render the DNA identification impermissible under the Fourth Amendment."[119] In 2014, the California Court of Appeals also recognized the distinction between DNA collection and DNA analysis when it stated, "[t]he collection of the DNA sample, however, is only the first part of the search . . . the second occurs when the DNA sample is analyzed and a profile created for use in state and federal DNA databases."[120]

Because GEDmatch's website contains a "terms of service" agreement, it must be considered whether the terms of that agreement waive a user's expectation of privacy in the DNA data he uploads to GEDmatch. GEDmatch's terms of service thoroughly warns its members that the site may be used by law enforcement to identify perpetrators of violent crimes.[121] GEDmatch further warns that its site may be used in a way that is not in line with its terms of service.[122] With that being said, the language within GEDmatch's warnings are simply that, and it is unclear whether these warnings alone would suffice as an express waiver of the user's privacy.[123] While any contractual issues between GEDmatch and its

[117] 59 F.3d 1556, 1564 (9th Cir. 1995).

[118] 690 F.3d 226, 243–44 (2012).

[119] 569 U.S. 435, 465 (2013). "CODIS. . . is the generic term used to describe the FBI's program of support for criminal justice DNA databases as well as the software used to run these databases. NDIS is considered one part of CODIS. . . ." FBI, *Questions*, *supra*, note 43.

[120] People v. Buza, 180 Cal. Rptr. 3d 753, 762–63 (Cal. Ct. App. 2014), *rev'd* 413 P.3d 1132 (Cal. 2018).

[121] *See supra* notes 73–74, 77–78 and accompanying text.

[122] *Id.*

[123] GEDMATCH, *supra* note 9. GEDmatch's privacy notice states, "if you require absolute privacy and security, you agree that you will not provide your personal information, Raw Data, or Genealogy Data to GEDmatch. If you do not agree and you have already provided your personal information, Raw Data, or Genealogy Data, you agree to

members are beyond the scope of this article, it is also important to note that GEDmatch did not update its terms of service to include these warnings until *after* the news about its use in identifying DeAngelo went public.[124]

Applying the first step of Justice Harlan's "reasonable expectation of privacy" test, there must be a subjective "actual expectation of privacy" to the DNA data uploaded onto GEDmatch or similar websites.[125] One privacy concern that supports the idea that there is an actual expectation of privacy in DNA data posted online for genealogical research is that DNA is shared between multiple people.[126] Thus, even if the GEDmatch member waives his expectation of privacy under GEDmatch's TOS,[127] he cannot waive the privacy rights of his relatives, who, by the communal nature of DNA, are exposed to the same level of government intrusion without their consent.[128] Additionally, familial DNA searching on government databases at the federal and state levels is tightly regulated.[129] For example, Maryland and the District of Columbia have prohibited familial DNA searching by statute.[130] By contrast, access to GEDmatch is essentially unregulated, giving police free rein to access the massive amounts of DNA data available.[131]

Moreover, familial DNA searching on state or federal government databases uses genetic data already provided to the government; whereas on GEDmatch, police have access to genetic information they would otherwise not be privy to. Ironically, a convicted felon required to submit a DNA sample to the government may ultimately have more privacy than people

---

delete it immediately." *Id.*

[124] Murphy, *Family History Website*, *supra* note 11; *see also supra* note 72 and accompanying text.

[125] *See supra* note 98–99 and accompanying text.

[126] Murphy, *Relative Doubt*, *supra* note 13, at 317.

[127] GEDMATCH, *supra* note 9.

[128] Editorial Board, *Golden State Killer Case Raises Legal and Ethical DNA Issues*, 44 CONN. L. TRIB. 46 (2018).

[129] Glen Martin, *Gird your Genes: What DNA Matching Might Mean for your Privacy*, CAL. MAG., July 24, 2018, https://alumni.berkeley.edu/california-magazine/just-in/2018-07-24/gird-your-genes-what-dna-matching-might-mean-your-privacy.

[130] *See supra* note 50 and accompanying text.

[131] Martin, *supra* note 129.

using GEDmatch for personal genealogical research.[132] As previously mentioned, the STR "junk genes" have little value other than for identification purposes.[133] However, the data on GEDmatch easily provides law enforcement agencies with access to an array of genetic information that goes far beyond identification, such as an individual's medical risks and predispositions.[134] The Supreme Court addressed this distinction and potential privacy concerns through dicta in *Maryland v. King*.[135] Arguably, the Court left the door open to future discussion on DNA analysis when it acknowledged the possible privacy concerns regarding governmental DNA analysis.[136] Theoretically, the government's unregulated use of GEDmatch is a way for law enforcement to evade too tight regulations and procedures that come with searching government DNA databases without invoking Fourth Amendment protections.[137] This exploitation in science and technology is precisely what the Supreme Court has warned against throughout its rulings on Fourth Amendment issues.[138]

Additionally, law enforcement's ability to obtain DNA data through GEDmatch is analogous to cell phone data discussed in *Riley v. California*.[139] In *Riley*, the Supreme Court, in recognizing a cell's phone's ability to hold large amount of information, stated that because "a significant majority of American adults now own such phones" containing "vast quantities of personal information," subjecting cell phones to a traditional search incident to arrest would be a greater intrusion into individual privacy.[140] Similarly, because an individual's SNP profile contains an immense amount of personal information, not only about that individual but about his family members, such a search would be a substantial intrusion into the individual's and his family member's privacy.[141]

---

[132] *Id.*
[133] Murphy, *Policy Oversight*, *supra* note 31, at e5.
[134] *Id.*
[135] 569 U.S. 435, 464 (2013); *see* quoted text *infra* p. 31.
[136] *Id.*
[137] *Id.*
[138] *See supra* notes 107–111 and accompanying text.
[139] 134 S. Ct. 2473 (2014).
[140] *Id.* at 2484–85.
[141] *See supra* notes 46–47 and accompanying text.

Nonetheless, a stumbling block to this analogy is that while the information within a person's DNA profile *is* communal in nature, familial searching on GEDmatch does not release an individual's complete raw DNA data to law enforcement.[142] The search results reveal only the small portion of the data that is shared between the two members.[143] Unlike a cell phone, which is direct access to an indefinite amount of information, a familial search on GEDmatch will reveal tiny portions of DNA information *only if* they match the DNA sample.[144] Furthermore, only the person who is in possession and has an ownership interest in the cell phone at the time of the arrest may claim a Fourth Amendment violation. Likewise, unless the defendant possessed a valid property interest in the DNA data the police used to identify him, he too would not have standing to assert a Fourth Amendment violation.[145]

Under step two of Justice Harlan's approach, the "actual expectation of privacy" must be one that society deems "reasonable."[146] The Supreme Court considers reasonableness as the "ultimate measure of the constitutionality of a governmental search.[147] The government's interest must outweigh the amount the search intrudes on a person's "reasonable expectation of privacy."[148] Because law enforcement officials utilize GEDmatch as merely an investigative tool and the DNA profiles accessed are not actual suspects, the "special needs" test may apply.[149] The "special needs" test, as Justice Blackmun stated in his concurring opinion in *New Jersey v. T.L.O.*, requires "exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable . . . ."[150] A court will normally

[142] Ellen M. Greytak et al., *Privacy and Genetic Genealogy Data*, 361 SCIENCE 857, 857 (2018).

[143] *Id.*

[144] *Id.*

[145] *See infra* Part IV, Sections 2 and 3.

[146] *See supra* notes 98–99 and accompanying text.

[147] Maryland v. King, 569 U.S. 435, 447 (2013).

[148] *Id.* at 461.

[149] Amy A. Liberty, *Defending the Black Sheep of the Forensic DNA Family*, 38 HAMLINE L. REV. 467, 505 (2015).

[150] 469 U.S. 325, 351 (1985) (Blackmun, J., concurring).

use a balancing test to weigh the government's interest against the privacy intrusion.[151]

In applying this balancing test, the most prominent argument in support of law enforcement's use of familial DNA searching on GEDmatch and other genealogical databases is that it has proven to be a reliable tool for correctly identifying perpetrators of violent crimes.[152] While this weighs heavily in favor of governmental interests, there is a slippery-slope argument that familial DNA searching may be used for purposes beyond identifying suspects of violent crimes.[153] One concern is police will expand the use of familial DNA searching to identify perpetrators of non-violent crimes. To support that concern, a recent study revealed that 80% of the participants surveyed supported law enforcement's use of genetic websites, such as GEDmatch, when identifying perpetrators of violent crimes.[154] Conversely, when using genetic websites as a tool to identify perpetrators of non-violent crimes, that support significantly dropped to 39%.[155]

With that being said, it may be premature to make the inductive leap that law enforcement agencies will extend both their time and resources conducting familial DNA searches for non-violent offenders.[156] Additionally, proponents argue that law enforcement agencies can carry out procedures and regulations to prevent familial DNA searching from being used to find suspects of non-violent or less serious crimes.[157] For example, California, one of the first states allowing state law enforcement agencies to conduct familial DNA searches, created detailed protocols and limited

[151] King, 569 U.S. at 461.

[152] Liberty, *supra* note 149.

[153] Drake Bennett & Kristen V. Brown, *Your DNA is Out There. Do you Want Law Enforcement Using it?*, BLOOMBERG BUSINESSWEEK (Oct. 27, 2018, 5:00 AM), https://www.bloomberg.com/news/features/2018-10-27/your-dna-is-out-there-do-you-want-law-enforcement-using-it.

[154] Christi J. Guerrini, *Should Police Have Access to Genetic Genealogy Databases? Capturing the Golden State Killer and Other Criminals Using a Controversial New Forensic Technique*, 16 PLOS BIOLOGY (Oct. 2, 2018), https://journals.plos.org/plosbiology/article?id=10.1371/journal.pbio.2006906#pbio.2006906.ref016.

[155] *Id.*

[156] *See* Bucholtz, *supra* note 54 (describing the process for finding the "Golden State Killer" as a "painstaking, four-month process").

[157] *Id.*

searches for use in identifying perpetrators of particularly violent crimes only.[158]

Furthermore, advocates state that familial DNA searching is an identification tool only.[159] Investigators must still obtain a DNA sample from the individual, either voluntarily, through a warrant, or through abandoned DNA, and run it against the crime scene sample to confirm a match.[160] So long as police obtained the suspect's DNA through one of these lawful measures, how they originally found the suspect would likely never come out at trial.[161] However, even if the government's interests for conducting familial searching on genealogical databases outweigh the intrusion into a person's reasonable expectation of privacy, there are currently no regulations or safeguards in place to prevent the police from using this procedure to find suspects of non-violent or less serious crimes.[162]

Additionally, familial DNA searching, especially on a commercial database, has its own significant margin of error.[163] For example, in 2014, FBI agents falsely accused Michael Usry of committing a 1996 murder in Idaho Falls.[164] The FBI suspected Usry after his father's DNA and the killer's DNA partially matched, which ultimately was a false positive.[165] Similarly, in their hunt to identify the "Golden State Killer," familial DNA searching on GEDmatch first led investigators to the wrong suspect.[166]

---

[158] Alexandra Aherne, *Support of Familial DNA Testing in Illinois Criminal Investigation*, 38 N. ILL. U. L. REV. 553, 569 (2018); *Memorandum of Understanding Familial Searching Protocol*, CAL. OFF. ATT'Y GEN., https://oag.ca.gov/sites/all/files/agweb/pdfs/bfs/fsc-mou-06142011.pdf (last visited Nov. 21, 2018).

[159] Greytak, *supra* note 142.

[160] *Id.*

[161] Green, *supra* note 51.

[162] Murphy, *Policy Oversight*, *supra* note 31, at e6.

[163] *See* Avi Selk, *The Ingenious and 'Dystopian' DNA Technique Police Used to Hunt the 'Golden State Killer' Suspect*, WASH. POST (Apr. 28, 2018), https://www.washingtonpost.com/news/true-crime/wp/2018/04/27/golden-state-killer-dna-website-gedmatch-was-used-to-identify-joseph-deangelo-as-suspect-police-say/?utm_term=.4a0750b45b85 (stating that a 2014 British study found that familial DNA searches had an 83% failure rate).

[164] *Id.*

[165] *Id.*

[166] *Id.*

Authorities cleared the 73-year-old man only after obtaining a court-ordered buccal swab.[167] With a considerable risk of false positives, familial searching on websites such as GEDmatch can send law enforcement officers on a blind search, eerily reminiscent of colonial era "general warrants," only clearing an individual as a suspect after further intrusions into his privacy.[168] Courts would certainly have to take this level of intrusion into account when deciding whether the government's interests outweigh such an intrusion.

A second apprehension is that additional federal, state, or local government agencies may begin performing their own familial DNA searching on GEDmatch or similar websites, consequently leading to employment or insurance discrimination.[169] While this may become an increasing concern as technology advances in the field of genetics, there is not enough indication that genetic discrimination is currently a prevalent matter.[170] In addition, the Genetic Information Nondiscrimination Act (GINA) prevents health insurance companies from using or requiring genetic information to determine an individual's eligibility or coverage.[171] GINA also prevents employers from using or requiring genetic information in several aspects of an individual's employment.[172] However, GINA does not prevent all forms of insurance or employment genetic discrimination.[173] For example, GINA "does not protect against genetic discrimination in forms of insurance other than health insurance, such as life, disability, or

[167] *Id.*

[168] James Rainey, *Familial DNA Puts Elusive Killers Behind Bars. But Only 12 States use it*, NBC NEWS, (Apr. 28, 2018, 6:00 AM), https://www.nbcnews.com/news/us-news/familial-dna-puts-elusive-killers-behind-bars-only-12-states-n869711; *see supra* discussion Part III, p. 11–12.

[169] Benjamin E. Berkman et al, *Is it Ethical to use Genealogy Data to Solve Crimes?*, 169 ANN. INTERNAL MED. 333, 333 (2018).

[170] *Id.*

[171] 42 U.S.C.A. § 1320d-9 (Westlaw through P.L. 115-281); 42 U.S.C.A. 2000ff-1 (Westlaw through P.L. 115-281; *see generally* U.S. Nat'l Library of Med., *What is Genetic Discrimination?*, GENETICS HOME REFERENCE, https://ghr.nlm.nih.gov/primer/testing/discrimination (last visited Feb. 10, 2019) [hereinafter Library of Med., *Genetic Discrimination*] (defining genetic discrimination as employers or insurance companies treating people differently "because they have a gene mutation that causes or increases the risk of an inherited disorder").

[172] Library of Med., *Genetic Discrimination*, *supra* note 171.

[173] *Id.*

long-term care insurance."[174] Additionally, GINA is not applicable to those employer's with fewer than fifteen employees and does not protect U.S. servicemembers.[175]

Ultimately, should the Supreme Court recognize that an individual has a reasonable expectation of privacy when she posts her DNA data onto websites, such as GEDmatch, it will likely have to shift the way it currently views DNA analysis within the Fourth Amendment to encompass such broad protection.[176]

B. *Property Intrusion*

The Supreme Court's decision in *Jones* resurrected the property intrusion analysis under the Fourth Amendment.[177] If a property interest is linked to the DNA data used to identify the defendant, a familial DNA search on GEDmatch and similar genealogical databases may be considered a search under the Fourth Amendment.

Traditionally, courts held that a person retained no property interest in genetic material once it left his body.[178] For example, in *Moore v. Regents of the University of California*, researchers used tissue from Moore's spleen to patent a cell line.[179] When Moore filed suit for conversion of his genetic material, the California Supreme Court stated that Moore lacked a legal claim for conversion in his removed spleen tissue.[180]

Likewise, in *Greenberg v. Miami Children's Hospital Research Institute*, parents willingly provided genetic specimens to researchers studying a particular disease.[181] When researchers uncovered a genetic variation linked to the disease, both the researchers and the Hospital

[174] *Id.*

[175] *Id.*

[176] *See* Simmons, *supra* note 116, at 156 (stating that the Supreme Court considers a search under the Fourth Amendment as only the collection of data).

[177] *See supra* notes 101–102 and accompanying text.

[178] Ram, *supra* note 29, at 891.

[179] 793 P.2d 479, 481 (Cal. 1990).

[180] *Id.* at 488.

[181] Greenberg v. Miami Children's Hosp. Research Inst., 264 F. Supp. 2d 1064, 1067 (Fla. S.D. 2003).

patented the gene and related material.[182] Citing *Moore*, the district court dismissed the parents' conversion claim because they lacked the necessary property interest in the genetic material.[183] It is important to note that both of these cases involved donated genetic material, and the donation may have persuaded the courts that the parties had waived any property interests in the genetic material.[184]

However, a person's genetic/DNA data is separate and identifiable from the DNA specimen it derived from. As a result, there is a valid argument that property interests in the DNA data and the DNA specimen the data derived from are separate as well. While the Supreme Court has hinted that it may reject the idea that "genes are property," the Court has yet to tackle the question of whether *genetic data* is property.[185] In the state and federal district courts, there is a judicial trend, albeit slight, toward recognizing an individual's property right in his own DNA information.[186] For example, in *Peerenboom v. Perlmutter*, the Perlmutters asserted several claims, including a claim for conversion.[187] They alleged Peerenboom conspired to take the Perlmutters' genetic material.[188] In response to a motion to dismiss, a Florida judge ruled that "the Perlmutters enjoyed a property right in their genetic information, sufficient to state a claim for conversion."[189]

Likewise, in *Cole v. Gene by Gene, Ltd.*, a federal district court in Alaska denied Gene by Gene's motion to dismiss for lack of standing.[190]

---

[182] *Id.*

[183] *Id.* at 1074 ("Plaintiffs have no cognizable property interest in body tissue and genetic matter donated for research under a theory of conversion.")

[184] Ram, *supra* note 29, at 891 n.105.

[185] Ass'n for Molecular Pathology v. Myriad Genetics, Inc., 569 U.S. 576 (2013); *see also* Tufik Y. Shaveb, *You are What you Own: Reopening the Discussion on Universally Recognizing a Property right in Genetic Information and Material*, 38 WHITTIER L. REV. 181 (2017).

[186] Jessica L. Roberts, *Progressive Genetic Ownership*, 93 NOTRE DAME L. REV. 1105, 1109 (2018).

[187] Peerenboom v. Perlmutter, No. 2013-CA-015257 (Fla. Cir. Ct. Apr. 7, 2017).

[188] *Id.*

[189] *Id.*; Roberts, *supra* note 186, at 1109–10.

[190] Cole v. Gene by Gene, Ltd., 322 F.R.D. 500 (D. Alaska 2017), aff'd, 735 F. App'x 368 (9th Cir. 2018).

The plaintiff sued Gene by Gene for violating Alaska's Genetic Privacy Act.[191] In denying the motion to dismiss, the judge determined that the plaintiff established an exclusive property interest in genetic information.[192] In addition to Alaska, several other states have enacted legislation stating that an individual has a property interest in his genetic information.[193] Moreover, GEDmatch recognizes that its members have a property interest in their raw DNA data.[194] GEDmatch's TOS states, "Raw DNA data uploaded to GEDmatch.Com ('Raw Data') *remains the property* of the person who uploaded it."[195]

By applying the judicial trend and legislative action towards recognizing an individual's property interest in his own DNA data, along with GEDmatch's acknowledgement that its members retain their property interest in their DNA data, it is possible that law enforcement agencies violate that property interest upon accessing and using the individual's DNA data while conducting the familial search. However, this would violate only the privacy of the person retaining the property interest in the data and not necessarily the criminal defendant.

C. *Constitutional Standing*

An individual asserting a Fourth Amendment violation must also show that he has the standing necessary to assert his claim.[196] To do this, the defendant must show that the government violated his own expectation

---

[191] *Id.*

[192] *Id.* at 3.

[193] *See, e.g.*, COLO. REV. STAT. § 10-3-1104.7(1)(a) (LEXIS through 2018 Legis. Sess.) 2014) (stating that "genetic information is the unique property of the individual to whom the information pertains"); FLA. STAT. ANN. § 760.40(2)(a) (West, Westlaw through 2018 2d Reg. Sess. of 25th Legis.) (stating genetic testing results are "exclusive property of the person tested"); GA. CODE ANN. § 33-54-1(1) (LEXIS through 2018 Reg. Sess. of Gen. Assemb.) (stating that "genetic information is the unique property of the individual tested") OR. REV. STAT. ANN. § 192.537(1) (West, Westlaw through 2018 Reg. Sess. & 2018 Spec. Sess. of 79th Legis. Assemb.) (stating that "[a]n individual's genetic information and DNA sample are private and must be protected, and an individual has a right to the protection of that privacy").

[194] GEDMATCH, *supra* note 9.

[195] *Id.* (emphasis added).

[196] Rakas v. Illinois, 439 U.S. 128, 133–34 (1978).

of privacy.[197] Moreover, an individual may only assert his own rights in court and may not assert the rights of third parties.[198] For instance, in *Rakas*, the Supreme Court rejected the argument that a person automatically has standing to challenge a government search just because he was the "target" of such a search.[199] Similarly, a defendant identified through police conducted familial DNA search on GEDmatch would not have standing to challenge the constitutionality of the familial DNA search simply because he was the "target" of such a search.

Additionally, Fourth Amendment standing also limits the types of remedies available to the parties.[200] Most Fourth Amendment claims are asserted by the defendant in criminal trials where the remedy sought is excluding the unconstitutionally seized evidence, also known as the exclusionary rule.[201] However, in the context of GEDmatch, even if the criminal defendant could establish standing, the exclusionary rule would not be an adequate remedy. This is because the initial crime scene DNA was abandoned DNA left at the crime scene and not subject to Fourth Amendment protection.[202] Furthermore, the DNA obtained from the suspect, generally collected from a piece of trash, is also abandoned DNA not subject to Fourth Amendment scrutiny.[203] Therefore, there is nothing to exclude.

However, the owner of the DNA data used may have standing to assert a civil claim for the violations of her Fourth Amendment rights.[204] In that case, the owner may be able to seek either monetary damages or

[197] *Id.* at 140.

[198] David Gray, *The Fourth Amendment in the Digital Age: Collective Standing Under the Fourth Amendment*, 55 AM. CRIM. L. REV. 77, 86–87 (2018) ("There are, however, certain circumstances where the Court has allowed litigants to press claims *jus tertii*, meaning on behalf of absent third parties."). *C.f.* Rakas, 439 U.S. at 133–34 (stating that Fourth Amendment rights "may not be vicariously asserted").

[199] *Id.*

[200] Gray, *supra* note 198, at 95.

[201] *Id.*

[202] *See infa* Part V, Section 1.

[203] *Id.*

[204] *See* Rakas v. Illinois, 439 U.S. 128, 134 (1978) (stating that even a person who is not the defendant "may be able to recover damages for the violation of his Fourth Amendment rights or seek redress under state law for invasion of privacy or trespass") (citations omitted).

injunctive relief preventing law enforcement from conducting familial searches on GEDmatch and other genealogical research databases.[205] An injunctive relief remedy would require the DNA profile owner to show that there was a "real and immediate threat" that the police would again violate her Fourth Amendment rights by accessing her DNA profile on GEDmatch.[206]

Another possible solution to the Fourth Amendment standing issue is for the courts to adopt a version of the "cybersurveillance nonintrusion test" and apply it to familial DNA searching on genealogical research DNA databases.[207] This test, asserted by Margaret Hu as "implicitly suggested by the Supreme Court in *Jones*," shifts the analysis away from "an individual-based tangible harm inquiry to an inquiry of a society-wide intangible harm."[208] Accordingly, the burden shifts away from the individual to establish a reasonable expectation of privacy and puts the burden on the government to show why the surveillance of society is justified and necessary.[209] It also supports the argument that the Fourth Amendment goes beyond individual protection, allowing collective standing in Fourth Amendment constitutional issues.[210] This test can be adapted appropriately to include government familial DNA searching on genealogical databases, such as GEDmatch. The intertwined and communal nature of DNA combined with the technology to create extensive family trees with one partial DNA match makes it difficult to pinpoint a singular expectation of privacy. With enough time, manpower, and resources, the government has

[205] *See* Orin S. Kerr, *The Limits of Fourth Amendment Injunctions*, 7 J. ON TELECOMM. & HIGH TECH. L. 127, 131(2009) (stating that a court may grant injunctive relief in Fourth Amendment cases as long as the surrounding facts are established with "reasonable detail").

[206] *See* City of Los Angeles v. Lyons, 461 U.S. 95, 97–98 (1983) (holding that Lyons could not seek an injunction because he did not "establish a real and immediate threat that he would again be stopped for traffic violation, or for any other offense, by an officer or officers who would illegally choke him into unconsciousness without any provocation or resistance on his part").

[207] Margaret Hu, *Orwell's 1984 and a Fourth Amendment Cybersurveillance Nonintrusion Test*, 92 WASH. L. REV. 1819, 1830 (2017).

[208] *Id.*

[209] *Id.*

[210] Gray, *supra* note 198, at 100.

the unregulated ability to potentially identify an unknown number of Americans, who neither consented nor uploaded their own DNA profiles. It is certainly not unreasonable to shift the burden to the government to show why such an unregulated ability is reasonable. However, at this point, both the "cybersurveillance nonintrusion test" and the collective standing approach of the Fourth Amendment have not been adopted by the Supreme Court.

V. EXCEPTIONS TO THE FOURTH AMENDMENT SEARCH DOCTRINE APPLICABLE TO POLICE CONDUCTED FAMILIAL DNA SEARCHES ON GEDMATCH

Generally, the Supreme Court has considered acts defined as searches under the Fourth Amendment performed without a warrant as "per se unreasonable . . . subject only to a few specifically established and well-delineated exceptions."[211] While these exceptions are few, they prevent a wide variety of government conducted activity from invoking any Fourth Amendment scrutiny.[212] The exceptions that may be applicable to familial DNA searching on GEDmatch are each addressed in the sub-sections that follow

A. *Abandoned DNA*

While genetic material on a person is clearly subject to Fourth Amendment protection, once a person sheds genetic material from his body, it becomes "abandoned" and is generally exempt from any Fourth Amendment protection.[213] Likewise, the Supreme Court has held that there is no reasonable expectation of privacy in DNA recovered from someone's trash, and DNA obtained this way is not a search under the Fourth Amendment.[214] Just like DNA shed from a body, proponents of familial DNA testing on GEDmatch argue that once a person posts his DNA

[211] Arizona v. Gant, 556 U.S. 332, 338 (2009) (quoting Katz v. United States, 389 U.S. 347, 357 (1967)).

[212] Emily Berman, *When Database Queries are Fourth Amendment Searches*, 102 MINN. L. REV. 577, 595 (2017).

[213] Ferguson, *supra* note 101, at 594.

[214] California v. Greenwood, 486 U.S. 35, 41–42 (1988).

information online, any property interest is lost because it too has been "abandoned."[215] Since law enforcement agencies accessing DNA data on GEDmatch are not taking anything away from the individual, their use of GEDmatch does not trigger any Fourth Amendment protection.[216] Conversely, because the abandoned DNA principle applies only to the DNA *specimen*, acknowledging that there is a separate property interest in DNA *data* proposes a compelling argument that this Fourth Amendment exception should not apply.[217]

B. *Third-Party Doctrine*

The third-party doctrine states there is no reasonable expectation of privacy in information an individual voluntarily turns over to a third party, even when that information is used for limited purposes.[218] The rationale is that by turning information over to a third party, an individual "assumed the risk" that it could into the hands of the government.[219] Consequently, law enforcement agencies have generally been free to obtain third-party information without raising Fourth Amendment scrutiny.[220]

However, post *Carpenter*, the doctrine has lost some of its broad scope.[221] For example, records stored by a third party are no longer automatically immune from Fourth Amendment scrutiny simply because of its third-party status.[222] In *Carpenter*, the Supreme Court carved out a narrow exception to the third-party doctrine when it held that police-obtained cell-site location information (CSLI), information wireless phone companies collected and stored for purposes of improving the wireless networks and applying roaming charges, was a search under the Fourth

[215] Green, *supra* note 51.

[216] *Id.*

[217] *See supra* Part IV, Section 2.

[218] Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 443 (1976).

[219] Miller, 425 U.S. at 443.

[220] Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018).

[221] Susan Freiwald & Stephen Wm. Smith, *The Carpenter Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 230 (2018).

[222] *See* Carpenter, 138 S. Ct. at 2217 (stating that the fact CSLI records held by a third-party does not by itself overcome a claim to Fourth Amendment protection due to the uniqueness of the records).

Amendment.[223] In the majority opinion, Chief Justice Roberts stated that people "compulsively carry a cell phone with them all the time . . . . Accordingly, when the government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user."[224]

As it stands today, *Carpenter's* narrow third-party exception would not automatically extend to individuals uploading raw DNA data to GEDmatch or similar databases, but the holding is consistent with the Court's steadily shifting view on technology invading a "reasonable expectation of privacy."[225] The ruling in *Carpenter* likely foreshadows the Court's willingness to extend its holding to future cases involving familial DNA searching on genealogical databases because there are undeniable similarities between CSLI data and DNA data. First, both CSLI data and DNA are unique in nature and contain potentially sensitive information.[226] Second, prior to the Court's ruling, law enforcement agencies had unlimited access to CSLI data just as they currently do with DNA data on genealogical research databases.[227] Moreover, Chief Justice Roberts peppered the majority opinion in *Carpenter* with warnings about overreaching government intrusion due to advances in technology and science.[228]

In addition, online genealogy services, such as GEDmatch, along with other types of mass data collection, introduces the theory of "Fourth Party Consent."[229] Unlike the third-party doctrine where one party knows or assumed the risk that by giving his information to a third party, that

[223] *Id.* at 2220.

[224] *Id.* at 2218.

[225] *See* discussion *supra* Part III.

[226] *See* Carpenter, 138 S. Ct. at 2217.

[227] *Id.* at 2223 ("We decline to grant the state *unrestricted access* to a wireless carrier's database of physical location information.") (emphasis added).

[228] *See Id.* ("Here 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 . . . drafted the Fourth Amendment to protect.").

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

information may find its way to the government, a "fourth party" situation occurs when the government obtains a person's information from a third party, but the owner never consented to have his information submitted to that third party.[230] An individual cannot waive his expectation of privacy when he never consented to the release of his information.[231] Again, an analogy can be made to cell phone CSLI data. In *Carpenter*, the Court reasoned that because a cell phone user has no control over the generated CSLI data, he cannot voluntarily assume the risk of that information ending up in the hands of a third party.[232] Likewise, a person has no control over the amount of DNA he shares with a family member and cannot voluntarily assume the risk that his DNA data may be accessed through an online familial DNA search. If courts adhere to the principle that a fourth party may not waive his expectation of privacy when information is released to a third party without his knowledge or consent, this would protect the communal nature of DNA.

VI. WHERE DO WE GO FROM HERE?

While familial DNA searching is not a new process, law enforcement agencies conducting familial DNA searching on non-governmental databases is.[233] The courts will have to analyze several factors, with the most significant factor being that police are no longer searching "junk" DNA strands but DNA strands overflowing with private genetic information. When addressing this distinction in *Maryland v. King*, the Supreme Court stated:

> [T]he CODIS loci come from noncoding parts of the DNA that do not reveal the genetic traits of the arrestee. While science can always progress further, and those progressions may have Fourth Amendment consequences, alleles at the CODIS loci "are not at present revealing information beyond

[230] Jennifer Huddleston Skees, *Come Back with a Warrant: The Potential Impact of the Carpenter Decision Beyond Cell Phones*, PLAINTEXT.COM (July 27, 2018), https://readplaintext.com/come-back-with-a-warrant-the-potential-impact-of-the-carpenter-decision-beyond-cell-phones-a307f864b64d.

[231] *Id.*

[232] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

[233] *See supra* note 53 and accompanying text.

> identification." The argument that the testing at issue in this case reveals any private medical information at all is open to dispute.[234]

Additionally, the Court recognized that the Maryland statute prohibited law enforcement from performing testing beyond identification.[235] As mentioned before, there are no safeguards in place that limit how the police may use GEDmatch. As the Court hinted, this may very likely raise the need for a heightened level of Fourth Amendment scrutiny.[236] The privacy concerns surrounding law enforcement's use of genealogical DNA databases, like GEDmatch, are compelling and should not be disregarded.

Nonetheless, until there is a major shift in Supreme Court precedent it is unlikely that any defendant identified through familial searching on GEDmatch would have the necessary standing to assert a Fourth Amendment claim. At best, the owner of the DNA profile accessed and used may have standing to bring a civil claim, but he would be limited by the third-party exception to the Fourth Amendment because the holding in *Carpenter* would not extend to this situation.[237] Should a broader exception to the third-party doctrine occur in the near future, the profile owner may then have a private claim where an adequate remedy would be either monetary damages or an injunction.[238] However, should the DNA profile owner have standing to file a claim seeking an injunction, a *nationwide* injunction preventing *all* law enforcement agencies from conducting familial searching on GEDmatch and other genealogical databases would be unlikely.[239]

In the meantime, the most efficient way to limit law enforcement's use of GEDmatch and other genealogical research databases is to create and

---

[234] 569 U.S. 435, 464 (2013) (citations removed).

[235] *Id.* at 465.

[236] *See supra* note 162.

[237] *See* Carpenter v. United States, 138 S. Ct. 2206, 2209–10 (2018) (discussing that the Court's decision not to extend the third-party doctrine to cell-site records is narrow and does not include matters not before the Court).

[238] *See supra* note 204.

[239] *See* Haskell v. Harris, 745 F.3d 1269, 1271 (9th Cir. 2014) (stating that plaintiffs were free to seek a preliminary injunction from the trial court protecting a smaller class of people not included in the Supreme Court's holding in *Maryland v. King*).

enforce statutory and regulatory use restrictions.[240] For instance, the Maryland General Assembly recently proposed a bill expanding its prohibition on familial searching to include genealogical research databases.[241] With the immense privacy concerns and current lack of regulation, this article encourages legislation both at the state and federal level to promptly evaluate the risks and benefits of law enforcement's use of genealogical DNA databases and to respond proactively with appropriate legislative or regulatory measures. While a clear prohibition may be too extreme, statutory regulations restricting familial searching on genealogical databases only when all other investigative measures have been exhausted and limiting its use for cases involving only the most violent offenses, may strike a balance between the government's need to correctly identify perpetrators of violent crimes and the risks to individual's privacy.[242]

[240] Simmons, *supra* note 116, at 137–38.
[241] H.B. 30, 2019 Md. Gen. Assemb. (Md. 2019).
[242] See discussion on the balancing test, *supra* pp. 19–20.