William & Mary Law Review

Volume 61 (2019-2020)
Issue 1

Article 7

10-2019

Standing to Challenge Familial Searches of Commercial DNA Databases

Hillary L. Kody

STANDING TO CHALLENGE FAMILIAL SEARCHES OF COMMERCIAL DNA DATABASES

TABLE OF CONTENTS

INTRODUCTION

In April 2018, police officers arrested Joseph James DeAngelo.[1] DeAngelo, the officers claimed, was the "Golden State Killer," a man who committed dozens of murders and over fifty sexual assaults in California in the 1970s and 1980s.[2] The Golden State Killer had long eluded police, even though his DNA profile linked him to dozens of violent crimes.[3] While law enforcement officials from several jurisdictions in California had collected his DNA from crime scenes, the Golden State Killer's crimes predated modern DNA analysis.[4] Police found little use for the profile without a suspect's profile to compare to it.[5]

Nearly forty years later, the break in the case that ultimately implicated DeAngelo came when officers ran the Golden State Killer's DNA profile through an online genealogical DNA database, GEDMatch, and located a familial match—one of DeAngelo's third cousins.[6] Police traced DeAngelo through his family tree, eventually narrowing in on DeAngelo specifically.[7] Police then obtained DeAngelo's actual DNA sample by search warrant, and confirmed that DeAngelo and the Golden State Killer are one and the same.[8]

DeAngelo's apprehension and subsequent examples of police using similar tactics to solve cold cases—including the NorCal Rapist[9]—spurred a national debate on DNA and privacy.[10] Direct-to-

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 [https://perma.cc/EW8R-VU6U].

2. *Id.*

3. *See id.*

4. *Id.*

5. *See id.*

6. *See* Yaniv Erlich et al., *Identity Inference of Genomic Data Using Long-Range Familial Searches*, 362 SCI. 690, 690 (2018), http://science.sciencemag.org/content/sci/early/ 2018/10/10/science.aau4832.full.pdf [https://perma.cc/E3LT-65DA].

7. *Id.*

8. *See* Kolata & Murphy, *supra* note 1.

9. *See, e.g.*, Phil Helsel, *Police Use DNA to Arrest 'NorCal Rapist' Suspect in Crimes That Spanned 15 Years*, NBC NEWS (Sept. 22, 2018, 9:50 PM), https://www.nbcnews.com/news/us-news/police-use-dna-arrest-norcal-rapist-suspect-crimes-spanned-15-n912266 [https://perma.cc/JD57-M4LY].

10. *See, e.g.*, Tina Hesman Saey, *New Genetic Sleuthing Tools Helped Track Down the Golden State Killer Suspect: Mining Genealogy Databases to Find Crime Suspects Raises Pri-*

consumer DNA services, such as 23andMe and AncestryDNA, have dramatically expanded in recent years.[11] Over seven million at-home DNA kits were sold in 2017 alone.[12] As of April 2018, more than fifteen million people have undergone direct-to-consumer DNA testing.[13] Some scientists predict that 60 percent of Americans of European descent have a familial match as close as a third cousin in a commercial DNA database.[14]

Based on these statistics and the recent success tracking down the Golden State Killer and NorCal Rapist, police will likely see third-party DNA and ancestry databases as a valuable resource to assist in closing cold cases.[15] Law enforcement agencies across the country have thousands of unsolved cases involving DNA with no suspect profile to conduct a comparison.[16] But what are the Fourth Amendment implications of passing a perpetrator's DNA profile

---

vacy Concerns, SCI. NEWS (Apr. 29, 2018, 9:49 AM), https://www.sciencenews.org/article/golden-state-killer-suspect-dna-genetics-genealogy [https://perma.cc/2K93-FJ25]; 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 [https://perma.cc/A6LJ-DMZU]. In response to widespread media coverage of the Golden State Killer arrest, companies such as 23andMe published privacy statements reassuring users that their DNA information and data will not be released "without [the customer's] explicit consent." *Privacy*, 23ANDME, https://www.23andme.com/privacy/ [https://perma.cc/LRY3-SJ2Z]. However, 23andMe's website also states that information could be released if police present "a valid court order [or] subpoena." *Privacy Highlights,* 23ANDME, https://23andme.com/about/privacy/ [https://perma.cc/26QP-QNSF].

11. 23andMe was founded in 2006 and has over ten million customers. *About Us*, 23ANDME, https://mediacenter.23andme.com/company/about-us/ [https://perma.cc/9S2E-GY7U].

12. *See* Erlich et al., *supra* note 6.

13. *Id.*

14. *Id.*

15. Reports indicate that FamilyTreeDNA, another direct-to-consumer DNA service, is allowing the FBI access to its two million genetic profiles on a case-by-case basis. *See* Kristen V. Brown, *A Major DNA-Testing Company Is Sharing Some of Its Data with the FBI. Here's Where It Draws the Line*, FORTUNE (Feb. 1, 2019), http://fortune.com/2019/02/01/genetic-testing-consumer-dna-familytreedna-fbi/ [https://perma.cc/K82K-2MCN]; *see also* Eric Levenson & Artemis Moshtaghian, *This Cold Case Is the First Genetic Genealogy Arrest To Go to Trial*, CNN (June 12, 2019, 2:52 PM), https://www.cnn.com/2019/06/12/us/cold-case-genetic-genealogy-washington/index.html [https://perma.cc/4RXB-WJCY] (discussing the recent conviction of William Earl Talbott II who police identified after running his DNA through an open source DNA database).

16. For an interactive map of open homicide cases in cities nationwide, see Wesley Lowery et al., *Where Killings Go Unsolved*, WASH. POST (June 6, 2018), https://www.washingtonpost.com/graphics/2018/investigations/where-murders-go-unsolved/ [https://perma.cc/4UJ7-EJCJ].

through an ancestry database or compelling a third-party company to do so? Is such a process considered a search or does it otherwise implicate an expectation of privacy sufficient to trigger the warrant requirement of the Fourth Amendment? If this process constitutes a search, could an individual challenge the search of a family member's DNA profile if it eventually implicates them? This Note will address these questions.

In Part I, this Note will provide an overview of DNA and its use in criminal investigations and prosecutions. Part II will survey both the Supreme Court's third-party doctrine, including the Court's recent decision *Carpenter v. United States*, and the evolution of the Fourth Amendment "standing" doctrine.[17] Part III will compare DNA and cell-site location information, which the Court analyzed in *Carpenter*, concluding that individuals have an expectation of privacy in their own DNA profile even when shared with a third party. In Part IV, this Note will push the concept of standing, arguing that the nature of DNA—specifically the interconnectedness of DNA among family members—should allow a related individual to challenge the legality of a search of his familial DNA. Part V will address counterarguments.

I. DNA AND THE FOURTH AMENDMENT

Today, deoxyribonucleic acid (DNA) analysis occupies an indispensable place in the criminal justice system—connecting suspects to the DNA they leave behind at crime scenes. Police in the United States first utilized DNA analysis in 1986.[18] Since that time, law enforcement officials have regularly relied on matching a suspect's

17. While the Supreme Court in *Rakas v. Illinois* purported to do away with separate standing inquiry, 439 U.S. 128, 139 (1978), Justices on the Supreme Court and lower courts regularly use the term "standing." *See* United States v. Salvucci, 448 U.S. 83, 85-97 (1980); United States v. Payner, 447 U.S. 727, 738 (1980) (Marshall, J., dissenting); United States v. Kember, 648 F.2d 1354, 1365-66 (D.C. Cir. 1980). This Note will utilize the term "standing" as well.

18. *See* KEITH INMAN & NORAH RUDIN, AN INTRODUCTION TO FORENSIC DNA ANALYSIS 21 (1997). Before law enforcement agencies possessed the technology to analyze DNA, they often resorted to blood typing. *Id.* at 6-7. Beginning in the early 1970s, scientists could determine if a suspect's blood sample was of the same blood type as the one found at the crime scene. *Id.* at 7. Blood typing could help police eliminate suspects. *See id.* at 7-8. However, blood typing lacked the level of individual specificity of later DNA analysis. *See id.*

DNA profile to a DNA sample.[19] Courts have responded to the pervasive DNA collection and use as evidence, laying some groundwork for consideration of DNA under the Fourth Amendment.[20]

A. Basics of DNA and DNA Fingerprinting

Almost all human cells contain, in their nuclei, forty-six chromosomes made up of DNA.[21] Individuals inherit one half of their chromosomes from each of their parents.[22] DNA is made up of individual molecules known as nucleotides.[23] Four types of nucleotides—adenine (A), thymine (T), guanine (G), and cytosine (C)—in sequence form one half of a strand of DNA.[24] The DNA sequence matches up with a complementary sequence to form a DNA strand.[25] When matching up nucleotides, A always pairs with T, and G always pairs with C.[26] These couplings are known as "base pairs."[27] Base pairs form the basic structure of DNA, known as the "double helix."[28]

For genetic identification purposes, analysts look to identifiable patterns in the genetic code, known as short tandem repeats (STRs).[29] Individual STRs, averaging between two to five base pairs, form a sequence which repeats a set number of times.[30] STRs occupy

---

19. *See id.* at 21. The popular portrayal of DNA's use in television and movies may contribute to "the CSI effect"—the trend that juries expect prosecutors to present DNA evidence at any criminal trial. *See generally* Simon A. Cole & Rachel Dioso-Villa, *CSI and Its Effects: Media, Juries, and the Burden of Proof*, 41 NEW ENG. L. REV. 435 (2007); Kimberlianne Podlas, *"The C.S.I. Effect": Exposing the Media Myth*, 16 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 429 (2006).

20. *See infra* Part I.B.

21. *See* Henry T. Greely et al., *Family Ties: The Use of DNA Offender Databases to Catch Offenders' Kin*, 34 J.L. MED. & ETHICS 248, 249 (2006).

22. *Id.*

23. *Nucleotides and Bases*, GENETICS GENERATION, http://knowgenetics.org/nucleotides-and-bases/ [https://perma.cc/F5W5-PSWF].

24. HENRY C. LEE & FRANK TIRNADY, BLOOD EVIDENCE: HOW DNA IS REVOLUTIONIZING THE WAY WE SOLVE CRIMES 3 (2003).

25. *Id.* at 3-4.

26. *Id.* at 3.

27. *Id.* at 4.

28. Greely et al., *supra* note 21, at 249.

29. *See id.* at 250.

30. LEE & TIRNADY, *supra* note 24, at 6.

a fixed point on a chromosome.[31] By looking at the location of the STRs on the chromosome[32] and the number of repetitions, analysts can compare one DNA sample to another.[33]

In order to compare DNA samples—a process called DNA fingerprinting—crime laboratories in the United States look to a set of twenty STRs.[34] The twenty STRs are known as "CODIS core loci," after the Combined DNA Index System, the FBI's national DNA database.[35] Although STRs vary significantly between individuals, they are not unique in and of themselves.[36] However, when the twenty loci are analyzed together, the profile is unique when compared to other full profiles.[37]

Once analysts identify the twenty markers, they compare them to other profiles to see how closely they match.[38] On average, two unrelated people will share, at most, two or three markers.[39] First degree relatives share, on average, about half of the twenty pairs.[40] By comparing all twenty markers, the probability of a false positive is very small.[41] An exact match indicates that the two samples came from the same individual.[42] A partial match indicates a familial connection.[43]

Commercial DNA companies, rather than looking just at the twenty STR markers, conduct different forms of analysis[44] that

31. Greely et al., *supra* note 21, at 250.

32. Each location tested is known as a locus (plural: loci).

33. *Id.*

34. *See id.* In 2017, the FBI added seven new markers to the original thirteen CODIS loci. Criminal Justice Info. Servs., *Combined DNA Index System (CODIS)*, FED. BUREAU INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis [https://perma.cc/8ZFH-68B4].

35. *See id.* For additional information about the CODIS database, see *infra* Part I.C.

36. *See* Greely et al., *supra* note 21, at 251.

37. *See id.* at 250.

38. *See id.*

39. *Id.*

40. *Id.*

41. *See id.*

42. *See id.* at 250. Identical twins would also be an exact match. *See id.*

43. *See id.*

44. For a description of the differences between different types of genetic testing, see *What's the Difference Between Genetic Testing Technologies?*, VERITAS (July 30, 2018), https://www.veritasgenetics.com/whats-difference-between-genetic-testing-technologies [https://perma.cc/THU9-V6JY]; *see also What Are Single Nucleotide Polymorphisms (SNPs)?*, NAT'L INST. HEALTH (June 25, 2019), https://ghr.nlm.nih.gov/primer/genomicresearch/snp [https://perma.cc/QN3J-D78U].

expose substantially more information. For example, AncestryDNA states that it uses "microarray-based autosomal DNA testing" to analyze over 700,000 locations of a person's genome.[45] Such analysis provides customers with genetic, ancestry, and medical information. Courts have not yet grappled with how this vast increase in access to information should interact with the Fourth Amendment.

B. How the Courts Have Treated DNA Under the Fourth Amendment

Most court decisions on DNA searches have concerned law enforcement collection of DNA from convicts, arrestees, and others in the presence of police. The Supreme Court weighed in on the issue of preconviction DNA collection in *Maryland v. King*.[46] The Maryland DNA Collection Act allowed law enforcement to take a cheek swab DNA sample from any "individual who is charged with ... a crime of violence or an attempt to commit a crime of violence; or ... burglary or an attempt to commit burglary."[47] After arresting King for assault, police took his DNA and uploaded it to their database.[48] King's DNA profile matched to DNA gathered from a six-year-old rape case, for which King was later convicted.[49] The Court held that the Fourth Amendment allowed police to collect DNA by cheek swab from a person arrested for a "serious offense."[50] The police's actions were reasonable, according to the *King* Court, because the government interest in identifying an arrestee outweighed the minimal intrusion to the individual.[51]

Maryland is not the only state that allows DNA collection from arrestees.[52] California, Texas, Virginia, and Louisiana are among states that require preconviction DNA collection from individuals

45. *Frequently Asked Questions*, ANCESTRYDNA, https://www.ancestry.com/dna/en/legal/us/faq#about-3 [https://perma.cc/C264-RC9G].

46. 569 U.S. 435, 442 (2013).

47. *Id.* at 443 (quoting MD. CODE. ANN. PUB. SAFETY § 2-504(a)(3)(i) (LexisNexis 2011)).

48. *Id.* at 441.

49. *Id.*

50. *Id.* at 465.

51. *Id.* at 446.

52. *See* Greely et al., *supra* note 21, at 250.

charged with felonies.[53] Lower courts have also wrestled with the scope of permissible DNA searches under the Fourth Amendment.[54]

C. CODIS and the Rise of Consumer DNA Databases

In 1990, the Federal Bureau of Investigation piloted CODIS to assist federal and state law enforcement agencies in solving violent crimes.[55] The DNA Identification Act of 1994 solidified the CODIS project by establishing the National DNA Index System to match DNA profiles to known offenders.[56] When law enforcement enters a DNA profile into the CODIS database, searches can return a full match or a partial match.[57] A perfect match indicates that the DNA sample came from the offender listed in CODIS.[58] A partial match, however, indicates that the crime scene DNA originated from a family member of that offender.[59]

In addition to law enforcement databases, third-party consumer databases hold growing numbers of DNA profiles. As of April 2018, more than fifteen million people had undergone direct-to-consumer DNA testing.[60] Some scientists already predict that 60 percent of searches for individuals of European descent will result in the match of a third cousin—the same level of connection in the Golden State Killer case.[61] With the popularity of direct-to-consumer DNA services—over seven million at-home DNA kits were sold in 2017

53. *Id.* Federal law also authorizes the Attorney General to collect DNA samples from individuals who are arrested or detained under the authority of the United States. *See* Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, § 1004(a)(1)(A), 119 Stat. 2960, 3085.

54. *See* United States v. Thomas, 736 F.3d 54, 61 (1st Cir. 2013) (holding that grand jury violated defendant's rights when it subpoenaed defendant's DNA without probable cause). *Compare* United States v. Davis, 690 F.3d 226, 239 (4th Cir. 2012) (finding that extraction of DNA from a defendant's clothing constituted a search), *with* Commonwealth v. Arzola, 26 N.E.3d 185, 194 (Mass. 2015) (finding that police extracting DNA from defendant's shirt was not a search), *and* Raynor v. State, 99 A.3d 753, 767 (Md. 2014) (finding that DNA testing sample defendant left on chair in police station was not a search).

55. Criminal Justice Info. Servs., *supra* note 34.

56. *See id.*

57. Greely et al., *supra* note 21, at 251.

58. *See id.*

59. *Id.*

60. *See* Erlich et al., *supra* note 6, at 690.

61. *Id.*

alone[62]—and the vast amount of knowledge contained within commercially analyzed DNA samples,[63] it is only a matter of time before any person in the United States can be identified through a familial search of a third-party DNA database. Courts will soon need to address the question of whether a familial DNA search in a third-party database intrudes on a family member's expectation of privacy and should therefore require a warrant.

II. THIRD-PARTY DOCTRINE, *CARPENTER*, AND STANDING

While courts have not yet faced these exact facts, the Supreme Court has considered an individual's privacy interests in information shared with third parties, and when the police can collect DNA samples. This Part provides an overview of relevant case law. Section A discusses the basics of the Fourth Amendment and the Court's third-party doctrine jurisprudence. Section B analyzes the recent decision in *Carpenter v. United States*. Finally, Section C details the Court's standing doctrine.

A. Third-Party Doctrine Before Carpenter

The Fourth Amendment bars the government from committing "unreasonable searches and seizures" and requires a warrant, or at a minimum probable cause to support such a search or seizure.[64] The Supreme Court has repeatedly affirmed that the foundation of the Fourth Amendment is reasonableness.[65] Therefore, if a search is "reasonable," it is constitutionally permissible.[66]

---

62. *Id.*

63. *See supra* notes 44-45 and accompanying text.

64. The Fourth Amendment of the Constitution states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

65. *See, e.g.*, Fernandez v. California, 571 U.S. 292, 298 (2014); Brigham City v. Stuart, 547 U.S. 398, 403 (2006).

66. *See Fernandez,* 571 U.S. at 298; *Brigham City*, 547 U.S. at 403.

The modern test for constitutionally permissible searches stems from Justice Harlan's concurrence in *Katz v. United States*.[67] In interpreting the majority's holding, Justice Harlan envisioned a "twofold requirement" for Fourth Amendment reasonableness.[68] First, under the subjective requirement, the individual must have an actual expectation of privacy.[69] Second, under the objective requirement, that expectation of privacy must "be one that society is prepared to recognize as 'reasonable.'"[70] If an individual can meet both the subjective and objective elements, he has a reasonable expectation of privacy.[71] When the government violates a person's reasonable expectation of privacy, then it has violated his Fourth Amendment rights.[72]

The reasonable expectation of privacy calculus, however, is turned on its head when third parties are involved. In *United States v. Miller*—largely considered the beginning of the "third-party doctrine"—the Court held that Miller had "no protectable Fourth Amendment interest" in documents the government subpoenaed from his bank while investigating him for tax evasion.[73] The Court later stated that an individual has "no legitimate expectation of privacy in information he voluntarily turns over to third parties,"[74] even if the individual conveys that information expecting it to be used for a specific, limited purpose.[75] The third-party doctrine rests on the assumption that in providing information to a third party, an individual considered the increased likelihood that the third party may, intentionally or otherwise, share that information.[76] Therefore, in making the decision to provide information to a third party, the individual assumed this additional risk.[77]

Many scholars have criticized the third-party doctrine as being inconsistent with the Fourth Amendment generally, and the Court's

67. *See* 389 U.S. 347, 361-62 (1967) (Harlan, J., concurring).
68. *Id.* at 361.
69. *Id.*
70. *Id.*
71. *See id.*
72. *See id.*
73. 425 U.S. 435, 436-37 (1976).
74. Smith v. Maryland, 442 U.S. 735, 743-44 (1979).
75. *See Miller*, 425 U.S. at 443.
76. *See Smith*, 442 U.S. at 745; *Miller*, 425 U.S. at 443.
77. *See Smith*, 442 U.S. at 745; *Miller*, 425 U.S. at 443.

holding in *Katz* specifically.[78] This Note does not take up this argument. The Court has repeatedly affirmed the third-party doctrine, entrenching it in Fourth Amendment jurisprudence.[79] Instead, this Note considers the Supreme Court's latest examination of the third-party doctrine, articulated in *Carpenter v. United States*.[80] It then applies the *Carpenter* Court's analysis to DNA held in third-party databases.[81]

B. Carpenter v. United States *and Cell-Site Location Information*

In *Carpenter v. United States*, the Court considered whether the practice of obtaining cell-site location information (CSLI) from a third-party company was a Fourth Amendment search.[82] The defendant in *Carpenter* was convicted of multiple counts of robbery and carrying a weapon in commission of a federal crime of violence in connection with the series of robberies.[83] After a tip from a co-conspirator, investigators obtained a court order for Carpenter's cell phone records—including his CSLI—pursuant to a provision in the Stored Communications Act.[84] Under the Act, the government can force communications companies, such as cell phone providers, to disclose telecommunication records after receiving a court order.[85] Unlike a search warrant, which mandates probable cause, the Act only requires the government to have "reasonable grounds to believe" that the records contain information relevant to an ongoing

78. *See, e.g.*, 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.7(b)-(c) (5th ed. 2012); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 976-77 (2007) (articulating how and when individuals have an expectation of privacy to information, regardless of whether it is held by third parties); Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229, 1230-31 (1983) (arguing that the problem with the third-party doctrine is that it focuses on guilty individuals rather than presuming innocence). *But see, e.g.*, Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 564-66 (2009) (highlighting two critical functions of the third-party doctrine: maintaining the "technological neutrality" of the Fourth Amendment and ensuring clarity in Fourth Amendment application).

79. *See, e.g.*, *Smith*, 442 U.S. at 745; *Miller*, 425 U.S. at 443.

80. *See infra* Part II.B.

81. *See infra* Part III.

82. *See* Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

83. *See id.* at 2212.

84. *See id.*

85. *See* 18 U.S.C. § 2703(c)-(d) (2012); *Carpenter*, 138 S. Ct. at 2212.

investigation.[86] In holding that this practice constituted a search, the Court evaluated both the Court's previous recognition of privacy in an individual's location information and its third-party doctrine jurisprudence.[87]

1. Privacy Interest in Location Information

The Court began its discussion by reaffirming a person's expectation of privacy in his physical location.[88] That privacy expectation, the majority posited, related both to the voluntariness of the transmission of location information and the degree of thoroughness of police surveillance.[89]

The *Carpenter* Court referenced its decision in *United States v. Knotts*, where it held that a beeper placed within a container purchased by the defendant's co-conspirator and used to track the co-conspirator's vehicle was not a search under the Fourth Amendment.[90] In applying Justice Harlan's test from his concurrence in *Katz v. United States*,[91] the Court found that a person did not have an objective, justifiable expectation of privacy to his location when "traveling in an automobile on public thoroughfares."[92] By traveling in public, the person was voluntarily conveying his movements and location to anyone who might want to look.[93] As a result, the beeper, the Court reasoned, provided law enforcement with no more information regarding Knotts's movements than traditional police surveillance.[94] The *Carpenter* Court noted, however, that the *Knotts* decision drew the line at traditional, "rudimentary" police surveillance.[95] The *Knotts* decision did not apply to more far-reaching methods, such as "twenty-four hour surveillance."[96]

86. § 2703(d).
87. *See Carpenter*, 138 S. Ct. at 2214-17.
88. *See id.* at 2217.
89. *See id.*
90. *See id.* at 2215; *see also* 460 U.S. 276, 285 (1983).
91. *See* 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
92. *Knotts*, 460 U.S. at 281.
93. *See id.* at 281-82.
94. *See id.* at 282.
95. *Carpenter*, 138 S. Ct. at 2215.
96. *See id.*

The *Carpenter* Court also discussed the decision in *United States v. Jones*, in which the Court considered the constitutionality of monitoring the location of an individual through a GPS tracking device illegally attached to his car.[97] While the *Jones* Court decided that the practice was unconstitutional on other grounds,[98] the *Carpenter* Court noted that five Justices were concerned about the means, length, and scope of GPS tracking by law enforcement.[99] In his concurrence in *Jones*, joined by Justices Ginsburg, Breyer, and Kagan, Justice Alito stated that, in an age where individuals carry cell phones and drive cars equipped with GPS devices, society's expectation of privacy might be evolving.[100] Additionally, Justice Alito discussed concerns about the length of location monitoring, stating that tracking "every single movement of [Jones's] car for a very long period" would constitute a search.[101] Justice Sotomayor agreed with Justice Alito's assessments regarding evolving expectations of privacy and long-term GPS monitoring.[102] Among the *Carpenter* Court's fundamental concerns about warrantless access to CSLI was the scope of access to personal information, particularly the accuracy and length of surveillance information police could acquire from CSLI.[103]

97. *See id.*; 565 U.S. 400, 402 (2012).

98. The *Jones* Court based its decision on the idea that officers had committed a trespass against the defendant when placing a GPS tracker on his car. *Jones*, 565 U.S. at 404, 410. Justice Scalia, writing for the Court, harkened back to *Olmstead v. United States*, stating that trespass still formed a separate ground for Fourth Amendment protection. *Id.* at 405. Five Justices, while concurring, disagreed with Justice Scalia's rationale. *Id.* at 413-14. (Sotomayor, J., concurring) (agreeing that the action was "a search within the meaning of the Fourth Amendment" but noting that "the Fourth Amendment is not only concerned with trespassory intrusions on property"); *id.* at 419 (Alito, J. concurring in judgment) (stating that the Court's holding was "unwise," "strains the language of the Fourth Amendment," "has little if any support in current Fourth Amendment case law," and was "highly artificial"). Because the *Jones* majority's rationale differed from established Fourth Amendment jurisprudence, the decision has narrow application.

99. *See Carpenter*, 138 S. Ct. at 2215.

100. *See Jones*, 565 U.S. at 429 (Alito, J., concurring).

101. *Id.* at 430.

102. *See id.* at 415 (Sotomayor, J., concurring).

103. *See Carpenter*, 138 S. Ct. at 2217-19.

2. Third-Party Doctrine

The *Carpenter* Court then considered how the third-party doctrine applied to CSLI. The Court first discussed *Miller*, recounting that Miller's checks were not confidential documents and were used for commercial purposes:[104] "Miller had 'take[n] the risk, in revealing his affairs to another, that the information [would] be conveyed by that person to the Government.'"[105] The defendant in *Smith* likewise maintained little expectation of privacy in the phone numbers he dialed.[106] Therefore, the government's collection of those records did not constitute a search.[107] Further, both Smith and Miller had voluntarily conveyed this information to the third party.[108] In choosing to provide the information to a third party, Smith and Miller "assumed the risk" that the records would be shared.[109]

3. Expectation of Privacy & Third-Party Doctrine: The Court's Application in Carpenter

Despite these precedents, the Court did not extend the third-party doctrine to CSLI, finding that "an individual maintains a legitimate expectation of privacy in his physical movements as captured through CSLI."[110] Therefore, police acquisition of CSLI constituted a search subject to the Fourth Amendment.[111]

The Court first applied the *Katz* formulation, considering both subjective and objective expectations of privacy.[112] Citing *Jones*, the Court reasoned that society presumed that law enforcement officials could not "secretly monitor and catalogue" all of an individual's movements "for a very long period."[113] Procurement of CSLI directly violated this societal expectation.[114]

104. *See id.* at 2216.
105. *Id.* (quoting United States v. Miller, 425 U.S. 435, 443 (1976)).
106. *See id.*
107. *See id.*
108. *See id.*
109. *Id.*
110. *Id.* at 2217.
111. *See id.*
112. *See id.* at 2217-19.
113. *Id.* at 2217 (citing United States v. Jones, 565 U.S. 400, 430 (2012)).
114. *See id.*

In evaluating Carpenter's individual expectation of privacy, the Court further emphasized that time-stamped GPS data provided law enforcement access to deeply personal information about an individual's life.[115] Because everyone carries a cell phone, the government could access "near[ly] perfect surveillance" on almost any individual.[116] Further, by looking at historical CSLI, the government could virtually retrace a person's steps going back years.[117] The Court also noted the increasing capabilities of CSLI.[118] While CSLI technology may currently be "less precise than GPS information," it has become increasingly accurate.[119] Because "more sophisticated systems" were in development, the Court opted to adopt a rule which would cover these future advancements.[120] Therefore, both the present scope of CSLI and the future projected capability of similar technology constituted a level of intrusion into Carpenter's physical movements that he reasonably expected would remain private from the government.[121]

The Court distinguished CSLI from other information turned over to third parties both in terms of its scope and the voluntariness of its transfer.[122] In both *Smith* and *Miller*, constraints were present to limit the government's access to the individual's information.[123] CSLI, by contrast, had "no comparable limitations."[124]

---

115. *See id.* (citing *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)). In *Jones*, Justice Sotomayor explained how GPS tracking could generate a detailed description of an individual, allowing police access to a person's "familial, political, professional, religious, and sexual associations." 565 U.S. at 415 (Sotomayor, J., concurring). The *Carpenter* Court expressed concern with exactly this comprehensive intrusion into a person's private life. *See Carpenter*, 138 S. Ct. at 2217-18.

116. *Carpenter*, 138 S. Ct. at 2218.

117. *See id.*

118. *See id.* at 2219.

119. *See id.* at 2218.

120. *See id.* at 2218-19 (quoting Kyllo v. United States, 533 U.S. 27, 36 (2001)).

121. *See id.* at 2219.

122. *See id.* at 2217-18.

123. *See id.* at 2219. In *Smith*, the pen register contained call logs, thereby revealing minimal information regarding the caller's identity. *See id.*; Riley v. California, 134 S. Ct. 2473, 2492 (2014). Likewise, in *Miller*, the checks were "not confidential communications," and only used for "commercial transactions." United States v. Miller, 425 U.S. 435, 442 (1976); *see also Carpenter*, 138 S. Ct. at 2219. Neither Miller nor Smith had a reasonable expectation of privacy to the contents of these documents. *See Carpenter*, 138 S. Ct. at 2219; Smith v. Maryland, 442 U.S. 735, 743-44 (1979); *Miller*, 425 U.S. at 437.

124. *Carpenter*, 138 S. Ct. at 2219.

Access to CSLI thus allowed the government to possess expansive amounts of deeply personal and revealing information.[125]

Additionally, CSLI, although transmitted to the cell phone company, was not voluntarily shared in the same way Miller shared the checks with his bank or Smith shared his phone number with the pen register.[126] Practically everyone has a cell phone,[127] and it is nearly impossible to use a cell phone in accordance with societal expectations without constantly transmitting location information.[128] The average phone user, even if he is aware that he is transmitting location information to his phone company, cannot opt out.[129] Therefore, because Carpenter possessed a reasonable expectation of privacy in his physical location and the third-party doctrine did not apply, "the [g]overnment must generally obtain a warrant supported by probable cause" in order to acquire his or another individual's CSLI.[130] This same rationale likely supports an expectation of privacy in other information held by third parties, including, as this Note argues, DNA information.[131]

C. "Standing" Doctrine

In order to bring a Fourth Amendment challenge, a party claiming a violation must have "a personal stake in the outcome of the controversy."[132] Any criminal defendant easily meets this requirement—he has an interest in avoiding conviction and the resulting

125. *See id.* at 2217.

126. *See id.* at 2220.

127. As of February 5, 2018, 95 percent of Americans owned a cellphone and 77 percent of Americans owned a smart phone. *Mobile Fact Sheet*, PEW RES. CTR., http://www.pewinternet.org/fact-sheet/ mobile/ [https://perma.cc/M3FR-QPUJ].

128. *See Carpenter*, 138 S. Ct. at 2220.

129. *See id.* ("Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data.").

130. *Id.* at 2221. Unfortunately for Carpenter, the Court's conclusion did not benefit him on remand. After the Sixth Circuit acknowledged that the FBI violated Carpenter's Fourth Amendment rights when it obtained his CSLI, the court held that it would not exclude the CSLI data because "the FBI agents relied in good faith on the [Stored Communications Act]." United States v. Carpenter, 926 F.3d 313, 314 (6th Cir. 2019). Therefore, Carpenter's criminal conviction remained. *Id.*

131. *See infra* Part III.

132. Baker v. Carr, 369 U.S. 186, 204 (1962).

sentence.[133] However, to assert a Fourth Amendment challenge, a criminal defendant must satisfy another requirement—the challenged violation must have been a violation of his own rights, rather than the rights of a third party.[134]

The Supreme Court redefined its view on standing in *Rakas v. Illinois*.[135] The Court held that in order to challenge an illegal search, the defendant must have a "legitimate expectation of privacy" in the area searched.[136] Justice Rehnquist stated that the concept of Fourth Amendment standing was "more properly subsumed under substantive Fourth Amendment doctrine," rather than a separate inquiry.[137]

The process of wrapping standing into a substantive Fourth Amendment expectation of privacy analysis embodied an innovation for the Court. Prior to *Rakas*, the Court required a threshold inquiry into whether an individual had "standing" before asking whether the search violated his Fourth Amendment rights.[138] In *Rakas*, the Court held that an individual could not challenge the search of a car in which he was merely a passenger.[139] A temporary passenger in another person's vehicle did not have a legitimate expectation of privacy in the areas of the automobile that the police searched, including the glove compartment and under the passenger's seat.[140]

---

133. *See* Alderman v. United States, 394 U.S. 165, 174 (1969) ("There is no necessity to exclude evidence against one defendant in order to protect the rights of another."); LAFAVE, *supra* note 78, § 11.3.

134. *See* Wong Sun v. United States, 371 U.S. 471, 492 (1963) ("The [unlawful] seizure of this heroin [from co-conspirator Toy] invaded no right of privacy of person or premises which would entitle Wong Sun to object to its use at his trial.").

135. 439 U.S. 128, 137-39 (1978).

136. *Id.* at 148.

137. *Id.* at 139.

138. *See, e.g.*, Jones v. United States, 362 U.S. 257, 267 (1960) (finding that anyone "legitimately on premises" had automatic standing to challenge a search). While Justice Rehnquist desired to collapse standing into the substantive Fourth Amendment inquiry, Justices on the Supreme Court and lower court judges regularly use the term "standing" to refer to an individual's ability to raise a Fourth Amendment challenge. *See supra* note 17.

139. *Rakas*, 439 U.S. at 148.

140. *Id.* The Court compared petitioner's legitimate expectation of privacy to other cases where the Court found standing. *Id.* at 149. In *Jones*, the Court held that because Jones was "legitimately on premises" where the search occurred, he had standing to challenge the search. 362 U.S. at 267. While the Court abandoned the "legitimately on premises" test in *Rakas*, *see* 439 U.S. at 147, the *Rakas* Court maintained that Jones had a legitimate expectation of privacy to his friend's apartment because he had permission to use the apartment, had a key, kept his possessions at the apartment, had "dominion and control" over the apart-

Two years later, the Court found that one defendant possessed no legitimate expectation of privacy in the purse of someone carrying his narcotics,[141] while another had no legitimate expectation of privacy in documents held by his bank officer.[142]

The Court next considered whether an individual had a legitimate expectation of privacy in another's home where he was a guest.[143] In *Minnesota v. Olson*, the Court held that an overnight guest had "a legitimate expectation of privacy in his host's home."[144] Such expectation of privacy does not require the guest to have complete dominion and control over his host's home.[145] The expectation of privacy, rather, is based in societal customs and understandings.[146] The host has an expectation of privacy in his own home which extends to his guests.[147] While only temporarily permitted on the premises, the guest in *Olson* had standing to raise a Fourth Amend ment challenge.[148]

Lastly, in *Minnesota v. Carter*, the Court came to the opposite conclusion after asking whether guests possessed a legitimate expectation of privacy when they were only on the premises for commercial purposes, for a relatively short time, and otherwise lacked

---

ment, and could exclude others. *Id.* at 149. Similarly, the *Rakas* Court characterized the defendant in *Katz* as maintaining a legitimate expectation of privacy when he "shut the door" to the telephone booth, "exclude[d] all others," and "paid the toll." *Id.* (citing Katz v. United States, 389 U.S. 347, 352 (1967)).

141. *See* Rawlings v. Kentucky, 448 U.S. 98, 106 (1980). In *Rawlings*, the petitioner placed his narcotics within the purse of his companion, Cox. *Id.* at 101. Rawlings sought to challenge the legality of the search of Cox's purse. *Id.* at 100, 103. While he owned the narcotics within the purse, the Court found that Rawlings did not have a legitimate expectation of privacy in the purse at the time of the search because "he had known [the purse's owner] for only a few days" and had no right to exclude others from the purse, had never "received access to [the] purse" previously, or had Cox's consent to obtain possession of the purse. *Id.* at 105.

142. United States v. Payner, 447 U.S. 727, 731-32 (1980). In *Payner*, the Court agreed with the district court's assessment that a U.S. law enforcement official "'knowingly and willfully participated in the unlawful seizure' of [Payner's banker's documents]." *Id.* at 730 (citing United States v. Payner, 434 F. Supp. 113, 120 (N.D. Ohio 1977)). However, because the conduct did not "invade[ ] *his* legitimate expectation of privacy," Payner did not have standing to challenge the seizure. *Id.* at 731-32.

143. *See* Minnesota v. Olson, 495 U.S. 91, 98 (1990).

144. *Id.*

145. *See id.*

146. *See id.*

147. *Id.*

148. *See id.*

connection to their host.[149] The guests in *Carter* gathered in the host's home for the sole purpose of bagging cocaine.[150] A police officer, after peering through the blinds and seeing the illegal activity, obtained a search warrant.[151]

Although the plurality found that respondents had no legitimate expectation of privacy, a majority of the Court's Justices, both concurring and dissenting, believed that most house guests would have standing to challenge such a search.[152] Justice Kennedy, in his concurrence, stated that "almost all social guests have a legitimate expectation of privacy ... in their host's home."[153] However, the specific fact pattern in *Carter*—particularly respondents' lack of connection to the home—drove Justice Kennedy to conclude that respondents had no legitimate expectation of privacy.[154] Likewise, Justice Breyer, concurring in the judgment,[155] and all three dissenting Justices, found that respondents had standing to challenge the search.[156]

In recent cases, the Court has repeatedly found that an individual has a legitimate expectation of privacy in his own vehicle,[157] in another person's rental car,[158] and in his location information held by a third party.[159] In the coming years, the Court will likely consider technology-augmented searches that implicate privacy interests in a way that the *Rakas* Court could not have imagined. As the Court evaluates these challenges, the Court's trend toward a more expansive understanding of expectation of privacy may support challenges

149. 525 U.S. 83, 91 (1998).

150. *Id.* at 86.

151. *Id.* at 85.

152. *See id.* at 99, 102, 103.

153. *Id.* at 99 (Kennedy, J., concurring).

154. *Id.* at 102.

155. *Id.* at 103 (Breyer, J., concurring). Justice Breyer, while finding that respondents had standing to challenge the search, determined that the officer committed no constitutional violation. *Id.*

156. *Id.* at 106 (Ginsburg, J., dissenting) ("[W]hen a homeowner ... personally invites a guest into her home [for any purpose], that guest should share his host's shelter against unreasonable searches and seizures.").

157. United States v. Jones, 565 U.S. 400, 405-06 (2012) (finding that real and personal property can provide a foundation for expectations of privacy).

158. Byrd v. United States, 138 S. Ct. 1518, 1524 (2018) (holding that an unauthorized driver "in otherwise lawful possession and control of a rental car" has standing to challenge the constitutionality of a search therein).

159. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

for many defendants—including a defendant challenging a familial DNA search of a third-party database.

III. DNA AND CSLI

The *Carpenter* Court cited the "unique nature" of CSLI as the reason that its collection did not fall under the third-party doctrine.[160] While the Court considered its decision to be "a narrow one,"[161] the Court's reasoning concerning both the expectation of privacy and the third-party doctrine can—and should—be applied to DNA contained within third-party databases.

A. Expectation of Privacy in DNA

DNA—or more specifically, the DNA profile that stems from a DNA sample—gains its privacy significance when attached to the individual.[162] Just as the CSLI in *Carpenter* only provided law enforcement with actionable information when combined with Carpenter's identity, DNA profiles are only useful to law enforcement when they know to whom the DNA belongs.[163] Stemming from the connection to an individual is the expectation of privacy—both that of the individual and that which society recognizes—in the collection of DNA samples and the information generated in a DNA profile. This expectation of privacy in DNA rests on multiple, long-held understandings: that people possess an expectation of privacy in their medical information, in confidential information, and in personally identifiable data, even when shared with third parties.

First, DNA information maintains an expectation of privacy as medical information. Genetic information has a wide variety of medical purposes. DNA can indicate an individual's genetic risk for

160. *Id.*

161. *Id.* at 2220 (noting that the *Carpenter* holding does not apply to "real-time CSLI," "tower dumps," "conventional surveillance techniques," or foreign intelligence and national security).

162. Presently, while investigators can determine whether a particular sample of DNA came from a male or female subject, DNA cannot be tied to an individual without comparing it to a known sample of that individual's DNA. *See* JOHN M. BUTLER, FORENSIC DNA TYPING: BIOLOGY, TECHNOLOGY, AND GENETICS OF STR MARKERS 113-15 (2d ed. 2005); *supra* notes 32-41 and accompanying text.

163. *See* BUTLER, *supra* note 162, at 113-15.

certain diseases, including Parkinson's Disease, dementia, or cancer.[164] DNA can also provide information about paternity of a child or bring to light other familial connections.[165] If an individual submitted his DNA profile to a third party for medical purposes, say for a genetic disease test, it is easy to definitively state that the DNA profile is medical information.

But what about individuals who send their DNA to a third-party company solely to determine their ancestry?[166] Although ancestry may seem distant from medical uses, a person's ancestry can have medical connotations.[167] Studies have linked certain haplogroups—genetic groups who share a common ancestor—to multiple diseases.[168] For example, a 2012 study found that British men belonging to a particular Y chromosome haplogroup—men who share a common male ancestor—were at an increased risk of developing coronary artery disease.[169] The study prompted the U.K.'s National Health Service to publish detailed information about haplogroups in an effort to educate potentially affected men.[170] Information that provides doctors and patients with resources to make informed medical decisions should fall directly within the category of medical

164. In 2017, the FDA approved 23andMe to provide genetic testing for ten diseases. Press Release, U.S. Food & Drug Admin., FDA Allows Marketing of First Direct-to-Consumer Tests That Provide Genetic Risk Information for Certain Conditions (Apr. 6, 2017), https://www.fda.gov/news-events/press-announcements/fda-allows-marketing-first-direct-consumer-tests-provide-genetic-risk-information-certain-conditions [https://perma.cc/RJR3-7VXY]. A year later, the FDA authorized the direct-to-consumer genetic testing for breast cancer. Press Release, U.S. Food & Drug Admin., FDA Authorizes, with Special Controls, Direct-to-Consumer Test that Reports Three Mutations in the BRCA Breast Cancer Genes (Mar. 6, 2018), https://www.fda.gov/news-events/press-announcedments/fda/authorizes-special-controls-direct-consumer-test-reports-three-mutations-brca-breast-cancer [https://perma.cc/59S4-QQ8F]. It is likely that direct-to-consumer genetic testing options will continue to expand.

165. *See* Robin Williams & Paul Johnson, *Inclusiveness, Effectiveness and Intrusiveness: Issues in the Developing Uses of DNA Profiling in Support of Criminal Investigations*, 33 J.L. MED. & ETHICS 545, 556 (2005); Amanda Pattock, Note, *It's All Relative: Familial DNA Testing and the Fourth Amendment*, 12 MINN. J.L. SCI. & TECH. 851, 870 (2011).

166. *See* Erlich et al., *supra* note 6, at 690.

167. *See* Andrew Smart et al., Debate, *Health and Genetic Ancestry Testing: Time to Bridge the Gap*, 10 BMC MED. GENOMICS, Jan. 9, 2017, at 1.

168. *See id.* at 3 (discussing various studies connecting haplogroups to specific diseases).

169. *See id.*

170. *See id.*

information. Therefore, DNA information satisfies the threshold inquiry even if a person seeks only to obtain ancestry information.[171]

Genetic information should also fit within the concept of medical information because of the potential future medical uses of DNA. While DNA presently can determine predisposition for disease, the information contained with a genetic profile is likely to become more accessible as technology progresses.[172] Scientists only began to understand genetic connections to disease a half century ago.[173] Today, genetic testing is available for over two thousand conditions.[174] There is no reason to doubt that scientists' understanding of DNA will continue to grow.[175] The increasingly expansive nature of DNA requires the adoption of a rule that is future-proof.[176] Just as the *Carpenter* Court considered the increasing accuracy of CSLI and GPS technology when holding that individuals have a reasonable expectation of privacy in CSLI, a court evaluating privacy interests in DNA should consider the rapidly changing capabilities of DNA analysis.[177] Such scrutiny would likely result in a finding that an individual should possess a reasonable expectation of privacy in DNA, whether it is medical information or not.

The federal government has recognized a right to privacy in medical and genetic information through legislation.[178] Additionally, the Supreme Court has also found fundamental rights to privacy related

171. Even if ancestry information is not a medical record, an individual may still possess a reasonable expectation of privacy in it sufficient to implicate the Fourth Amendment. *See* United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (detailing how the search in *Jones* provided police access to a person's "familial, political, professional, religious, and sexual associations"). Ancestry information could fall within Justice Sotomayor's concern about intimate familial information.

172. *See* BUTLER, *supra* note 162, at 115 (discussing the rapid growth of DNA technologies).

173. Asude Alpman Durmaz et al., *Evolution of Genetic Techniques: Past, Present, and Beyond*, BIOMED RES. INT'L, 2015, at 2.

174. *See id.* at 1.

175. *See id.* at 5.

176. *Cf.* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

177. *See id.*

178. When Congress passed the Genetic Information Nondiscrimination Act, it included "[g]enetic information" within the Health Insurance Portability and Accountability Act of 1996's definition of "health information." 42 U.S.C. § 1320d-9(a)(1) (2012); *see also* Natalie Ram, *Genetic Privacy After* Carpenter, 105 VA. L. REV. (forthcoming 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3265827 [https://perma.cc/U6E4-JYJQ].

to medical treatment and decisions.[179] While these rights have not been extended to medical information, the information exchanged between a doctor and patient in the process of making such a medical decision may be covered within the Court's understanding of privacy.

Further, the Court has recognized—both implicitly and explicitly—an expectation of privacy in confidential information and communications.[180] In *Miller*, the Court noted that Miller's checks were "not confidential communications."[181] The Court suggested that had Miller's checks been confidential, he may have had an expectation of privacy in them.[182] Further, common law and many state rules of evidence recognize a privacy privilege or a physician-patient privilege.[183] While there are some exceptions to this privilege (that is, fraud or other criminal acts), the privacy interest generally extends to all communications made for the purposes of treatment or diagnosis.[184] It is likely that individuals have a reasonable expectation of privacy in their health information, and by extension their DNA.

Finally, DNA information may be subject to heightened privacy standards due to evolving societal expectations surrounding data privacy. Some federal courts have recognized a constitutional right to information privacy since 1980.[185] Building on current accepted privacy standards, Professor Natalie Ram argues that "genetic data is sensitive, personal, and largely private."[186] She further asserts that the privacy policies of 23andMe and AncestryDNA support the fact that individuals have an expectation of privacy in DNA information shared with these companies.[187] Ram's viewpoint gains

179. Under its substantive due process jurisprudence, the Court has recognized a wide variety of privacy rights that implicate medical treatment or decisions. *See, e.g.*, Cruzan v. Dir., Mo. Dep't of Health, 497 U.S. 261, 280 (1990) (right to refuse life sustaining treatment); Roe v. Wade, 410 U.S. 113, 154 (1973) (right to choose whether or not to have an abortion); Griswold v. Connecticut, 381 U.S. 479, 485-86 (1965) (right to access contraception).

180. *See* United States v. Miller, 425 U.S. 435, 442 (1976).

181. *Id.*

182. *See id.*

183. 2 FED. EVID. PRACT. GUIDE § 10.07 (2019).

184. *See id.*

185. *See* United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980); *see also* Behar v. Pa. Dept. of Transp., 791 F. Supp. 2d 383, 393 (M.D. Pa. 2011).

186. Ram, *supra* note 178, at 26.

187. *Id.* at 50-54. Ram contrasts the privacy policies of 23andMe and AncestryDNA with GEDmatch and FamilyTreeDNA. *Id.* at 50-68. Ram states that "[w]hile 23andMe and

support from the five concurring and dissenting Justices in *Jones*, who noted the evolving societal expectations of privacy surrounding GPS location tracking.[188] Almost everyone carries a GPS tracker in their cell phone or has GPS in their car.[189] At the same time, GPS tracking continues to increase in accuracy—allowing an analyst to glean more information about a person's location than he could previously.[190] Mirroring this enhanced accuracy, society's expectation of privacy in location information has increased.[191]

In the same way, as more and more individuals contribute their DNA information to third-party databases, analysts can gather substantial amounts of information about an individual.[192] The potential scope of intimate information that an analyst or the government could recover from a DNA profile is substantially greater than that contained within location information.[193] As scientific understanding of genetics grows, a previously obtained DNA sample can provide more and more information about the individual.[194] Therefore, with improving technology, society's expectation of privacy in DNA information will likewise increase.

B. Involuntary Transfer of DNA

Like CSLI, DNA profiles contained within third-party databases would implicate an individual whether or not that individual himself conveyed the information to a third party.[195] Familial DNA searches allow police to obtain a partial, familial match to a DNA sample.[196] The third-party doctrine assumes that the individual

---

AncestryDNA take pains to emphasize their commitment to user genetic privacy, particularly vis-a-vis the government, GEDmatch has taken quite the opposite approach." *Id.* at 55.

188. *See* 565 U.S. 400, 429 (2012) (Alito, J., concurring) (joined by Justices Breyer, Ginsburg, and Kagan); *id.* at 415 (Sotomayor, J., concurring).

189. *See* Adam Cohen, *What Your Cell Phone Could Be Telling the Government*, TIME (Sept. 15, 2010), http://content.time.com/time/nation/article/0,8599,2019239,00.html [https://perma.cc/8WNS-5NA4]; *Mobile Fact Sheet*, *supra* note 127.

190. *See* Carpenter v. United States, 138 S. Ct. 2206, 2218-19 (2018).

191. *See Jones*, 565 U.S. at 429 (Alito, J., concurring).

192. *See* Durmaz et al., *supra* note 173, at 3.

193. *See id.*

194. *See id.*

195. *See* Erlich et al., *supra* note 6, at 690.

196. *See* Greely et al., *supra* note 21, at 250.

voluntarily provides information to a third party.[197] However, if there is no "voluntary exposure," then the rationale for the third-party doctrine disappears.[198] While a DNA profile in a third-party database may not be "indispensable to participation in modern society," for many Americans, "there is no way to avoid" sharing DNA information with a third-party database.[199] It is difficult to say, looking at the increasing likelihood that DNA information connected to an individual will soon exist within a third-party database regardless of any action taken by that individual,[200] that any given person has "assumed the risk."[201]

Even if an individual does voluntarily give over his DNA to a third party, it is unlikely that he understands the scope of the information he is sharing. The Court in *Miller* stated that even if an individual only reveals information "for a limited purpose" and in confidence, the Fourth Amendment does not preclude the government from obtaining that information.[202] However, in *Carpenter*, the Court considered that even though an individual may be aware that he is sharing his location information with his cell phone company, the scope of that sharing was beyond his control.[203] The *Carpenter* Court noted that the government's access to CSLI to track a person's location vastly increased its traditional surveillance ability.[204] The government, in effect, would have "absolute surveillance" capabilities.[205]

Similarly, the expansive, invasive nature of DNA information, even when voluntarily and knowingly provided to a third party, presents an incredible increase in the government's capabilities. Currently, law enforcement must collect and analyze a DNA sample before they can compare it to their suspect's profile.[206] Suspect pools

197. *See* Smith v. Maryland, 442 U.S. 735, 743-44 (1979); United States v. Miller, 425 U.S. 435, 443 (1976).

198. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

199. *See id.*; Erlich et al., *supra* note 6, at 690 (finding that the majority of white Americans currently have a third cousin DNA match in a third-party DNA database).

200. *See* Erlich et al., *supra* note 6, at 690.

201. *See Carpenter*, 138 S. Ct. at 2220; *Smith*, 442 U.S. at 745.

202. *Miller*, 425 U.S. at 443.

203. *Carpenter*, 138 S. Ct. at 2216-17.

204. *Id.* at 2218.

205. *Id.*

206. *See* INMAN & RUDIN, *supra* note 18, at 13-16.

are limited to law-enforcement-maintained databases, such as CODIS, or DNA samples collected during an investigation.[207] With access to a third-party DNA database, police can search vast cross-sections of the population's DNA.[208] "Only the few without" a third cousin or closer relative who has submitted DNA to a third-party database "could escape this tireless and absolute" search.[209]

C. Sufficient Safeguards and Comparable Limitations

Allowing the third-party doctrine to control DNA profiles held by third-party companies implicates the same concerns regarding the revealing nature of CSLI expressed in *Carpenter*. When collecting a DNA profile used for genealogical or medical testing purposes, there is no way for police to limit their inquiry to the particular information sought.[210] DNA profiles used for these purposes go beyond the "identifying information" in *Smith*.[211] Commercial companies test for about 600,000 variations of individual DNA letters.[212] Law enforcement utilizing DNA for identification purposes generally only analyze thirteen STRs.[213] A commercially tested DNA profile, therefore, contains significantly more information—allowing law enforcement officials to connect a DNA profile to more distant relatives.[214] Likewise, police could gain a vast amount of an individual's medical information[215]—going far beyond identification purposes that usually support DNA collection.[216] Police are unable to discriminate between "instruments ... used in commercial transactions" and "confidential communications" that inform medical or familial

207. *See supra* notes 50-59 and accompanying text.

208. *See supra* notes 60-63 and accompanying text.

209. *See Carpenter*, 138 S. Ct. at 2218; *see also* Erlich et al., *supra* note 6, at 690 (finding that 60 percent of Americans of European descent have a third cousin DNA match in a third-party database).

210. *See infra* notes 215-18 and accompanying text.

211. *See Carpenter*, 138 S. Ct. at 2219 (quoting Smith v. Maryland, 442 U.S. 735, 742 (1979)).

212. Saey, *supra* note 10.

213. Pattock, *supra* note 165, at 856.

214. *See* Saey, *supra* note 10.

215. *See* Durmaz et al., *supra* note 173, at 5.

216. *See, e.g.*, Maryland v. King, 569 U.S. 435, 450-51 (2013).

decision-making.[217] The same concerns underlying the *Carpenter* decision about CSLI—evolving expectations of privacy, involuntary transfer, and a lack of sufficient safeguards—apply equally to DNA.[218] Courts should therefore find that DNA profiles held by third-party companies should likewise be subject to the warrant requirement.

IV. STANDING TO CHALLENGE FAMILIAL DNA SEARCHES OF THIRD-PARTY DATABASES

Police tracked Joseph James DeAngelo through a familial DNA match.[219] If law enforcement found an exact match to an individual's DNA, that individual could certainly challenge the constitutionality of the police's search.[220] But what about a search of familial DNA that implicates an individual? Generally, a person cannot challenge a search that intrudes on another's expectation of privacy.[221] Recall that in *Rawlings v. Kentucky*, the defendant could not challenge the search of his companion's purse because—despite owning the contents of the purse—he did not have an expectation of privacy in the purse itself.[222]

Genetic information, however, differs drastically from physical property. DNA information is interconnected between family members.[223] Because a person inherits their DNA from their parents, it is impossible to fully separate a parent's DNA from his children's DNA or two biological siblings' DNA from one another.[224] The closer the familial relationship between two individuals, the more similar their DNA profiles are.[225] Therefore, even if police conducted a search on a family member's DNA, that DNA profile is

217. Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) (quoting United States v. Miller, 425 U.S. 435, 442 (1976)).

218. *See id.* at 2217-20.

219. Kolata & Murphy, *supra* note 1.

220. Courts allow defendants to challenge collection and analysis of their own DNA. *See, e.g.*, *King*, 569 U.S. at 465 (finding that police procedure to take a cheek DNA swab for identification purposes is reasonable).

221. *See supra* notes 132-40 and accompanying text.

222. *See* 448 U.S. 98, 105-06 (1980).

223. *See supra* notes 38-43 and accompanying text.

224. *See* Greely et al., *supra* note 21, at 250.

225. *See id.*

more connected to the individual than it would be to another randomly selected person.[226]

In this way, a DNA profile is more analogous to jointly held property. Generally, residents of a home,[227] tenants,[228] and even hotel room occupants[229] have standing to challenge a search. As long as an individual has a legitimate expectation of privacy, he will have standing.[230] Additionally, according to five Justices in *Minnesota v. Carter*, practically all house guests have a legitimate expectation of privacy in their host's home.[231] Almost any connection to the home would be sufficient for Justice Kennedy.[232] A guest, invited into a home for any purpose, could challenge a search under Justice Ginsburg's analysis.[233] By this reasoning, a homeowner's newest acquaintance or repeat drug dealer would have standing to challenge a constitutional violation.[234] This is a relatively expansive understanding of the expectation of privacy.

By contrast, a defendant challenging a familial DNA match would have a closer relationship to the individual who "owns" the searched DNA than any house guest would have with the host. Relatives can share up to half of their DNA with each other.[235] An individual's expectation of privacy in half of his DNA is more substantial than his expectation of privacy to his hotel room or the home of his acquaintance. This expectation of privacy in his familial DNA should,

---

226. *See id.*

227. *See, e.g.*, Wilson v. State, 330 S.E.2d 364, 367 (Ga. 1985) (finding that defendant had standing to challenge the search of his room at his grandmother's house).

228. *See, e.g.*, United States v. Vega, 221 F.3d 789, 797 (5th Cir. 2000) (finding tenant's possessory interest in property sufficient for standing).

229. *See, e.g.*, United States v. Domenech, 623 F.3d 325, 331 (6th Cir. 2010) (finding that defendant had standing to challenge search of hotel room he rented).

230. *See* Rakas v. Illinois, 439 U.S. 128, 143, 148-49 (1978).

231. *See supra* notes 152-56 and accompanying text.

232. *See* Minnesota v. Carter, 525 U.S. 83, 99-103 (1998) (Kennedy, J., concurring) (stating that while defendants "established nothing more than a fleeting and insubstantial connection [to their host's] home ... as a general rule, social guests will have an expectation of privacy in their host's home").

233. *See id.* at 106 (Ginsburg, J., dissenting) ("[W]hen a homeowner ... personally invites a guest into her home [for any purpose], that guest should share his host's shelter against unreasonable searches and seizures.").

234. *See id.*

235. *See* Greely et al., *supra* note 21, at 250. This number excludes identical twins, who share 100 percent of their DNA with one another. *Id.*

therefore, be sufficient for standing to challenge a search of it in a third-party database.

V. COUNTERARGUMENTS

The two chief arguments against standing to challenge familial DNA searches in third-party databases come from both sides. On the one hand, some argue that an individual has no privacy interest in another's DNA profile, and therefore should not be able to challenge a warrantless search of that profile. Others argue for a more expansive view of standing—that an individual should have standing to challenge any warrantless familial DNA search, including one of a police database.

A. A Person Has No Reasonable Expectation of Privacy in a Family Member's DNA

Scholar Amanda Pattock argues that the benefits of familial DNA testing to society outweigh the intrusion to an individual's privacy.[236] Law enforcement officials, Pattock suggests, have strong interests in identifying suspects, deterring crime, and more efficiently utilizing resources.[237] Individuals' interests include limiting exposure of familial secrets or otherwise embarrassing information and protection from overly intrusive law enforcement officials.[238]

In finding that the interests of society outweigh individuals' privacy interests, Pattock minimizes the individual's substantial privacy interests. However, as this Note details, an individual has numerous and considerable privacy interests in his genetic information.[239] Law enforcement officials certainly have interests in efficiently solving crimes and maintaining confidence in the criminal justice system.[240] But, even when engaging in a balancing test, efficiency and other policy concerns cannot support law enforcement intrusion into recognized and reasonable privacy interests of

236. Pattock, *supra* note 165, at 871.
237. *Id.* at 867-68.
238. *Id.* at 870-71.
239. *See supra* Part III.A.
240. Pattock, *supra* note 165, at 867-68.

individuals. This is exactly the concern underpinning the Court's reasonable expectation of privacy jurisprudence, and ultimately, the type of government intrusion that the Fourth Amendment was designed to protect against.[241] Thus Pattock's argument fails to stand because it does not give adequate weight to an individual's privacy interest in genetic information.

B. An Individual Has Standing to Challenge Any Familial DNA Search

Scholar Lina Alexandra Hogan argues that the "expanded use of [law enforcement-managed DNA databases] to include familial searches is a serious intrusion into family members' expectations of privacy."[242] In arguing that a family member should have standing to challenge any familial search of a *police* (as opposed to a third-party) DNA database, Hogan concludes that a family member's privacy interests outweigh the government's interests, thereby making a familial DNA search unreasonable.[243] This Note agrees with Hogan's analysis regarding the intimate relationship between family members' DNA.[244] As Hogan says, "Genetic information is the most intimate and private information."[245] Further, it is impossible to disassociate an individual's DNA from his family member's DNA.[246]

But this close relationship does not extend an expectation of privacy to the family member of a person whose DNA is held in a police database. The distinction between a familial search of police-controlled DNA and third-party controlled DNA comes down to the expectation of privacy in the underlying DNA sample. This Note previously determined that a person should have an expectation of privacy in his genetic profile held by a third party.[247] Most individuals who provide DNA to a third-party company do so for medical

241. *Cf.* Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018).

242. Lina Alexandra Hogan, Note, *Guilt by Relation: If Your Brother Is Convicted of a Crime, You Too May Do Time*, 30 W. NEW ENG. L. REV. 543, 586 (2008).

243. *See id.* at 584-85.

244. *See supra* Part IV.

245. Hogan, *supra* note 242, at 579; *see also supra* notes 210-18 and accompanying text.

246. *See* Hogan, *supra* note 242, at 571-74.

247. *See supra* Part III.

testing or ancestry determinations.[248] Society has long recognized special protections and privacy expectations in confidential medical information.[249]

In contrast, there is no similar privacy interest in a law enforcement database.[250] The Supreme Court concluded that an individual has a diminished expectation of privacy when in police custody.[251] This lowered expectation of privacy allows police to swab an arrestee's mouth for DNA without violating the Fourth Amendment.[252] Further, the Court has repeatedly suggested that a person's expectation of privacy is less when it concerns only identification information.[253] Unlike DNA that an individual turns over to a third-party company, there is likely little expectation of privacy to DNA collected by police for identification.

There is an additional component separating familial searches of police DNA databases from familial searches of third-party DNA databases—individuals are often aware of even distant family members' arrests. This is especially true for violent or serious crimes, when police can take DNA at the time of arrest.[254] By contrast, a person may not know that an immediate family member sent a DNA sample to a company for medical testing or ancestry analysis. People often keep medical diagnostics and information private from those closest to them.[255] Considering this, it is unreasonable to suggest that a third cousin would be aware that his relative had given DNA to a third-party company. The level of notice for family members of convicts and arrestees further distinguishes police-held DNA databases from third-party DNA databases. Due to the lack of underlying privacy interest, coupled with notice, an individual would have little foundation to support an expectation

248. *See supra* Part III.A.

249. *See supra* Part III.

250. *See* Maryland v. King, 569 U.S. 435, 463 (2013).

251. *See id.*

252. *Id.* at 463-64.

253. *See id.* at 461 ("[T]he Court must give great weight ... to the significant government interest [in identification of arrestees through DNA]."); Davis v. Mississippi, 394 U.S. 721, 727 (1969) (suggesting that "under narrowly defined circumstances," fingerprinting for identification may comply with the Fourth Amendment).

254. *See King*, 569 U.S. at 447-48.

255. *See supra* Part III.A.

of privacy argument sufficient for standing to challenge a police-maintained DNA database.

CONCLUSION

Familial DNA searches of third-party databases present uncharted territory for courts. If police continue to utilize results of these searches in criminal investigations, Fourth Amendment challenges will come. These future challenges to DNA searches of third-party databases will not be alone—they will join a myriad of other issues, such as warrantless collection of CSLI, confronting courts as technology strains former understandings of the scope of the Fourth Amendment.

Traditional understandings of both expectations of privacy and standing would preclude challenges to familial searches of DNA held by third parties.[256] However, as evidenced in part by the Court's decision in *Carpenter*, society's expectations of privacy are evolving.[257] Genetic information implicates data privacy, medical information, and confidentiality concerns.[258] Due to the unique, interconnected, and sensitive nature of DNA, an individual has a heightened and sufficient expectation of privacy.[259] Therefore, law enforcement must obtain a warrant before accessing DNA held by a third party.[260] This same expectation of privacy extends to family members who are unable to disconnect their DNA from their family members' DNA in third-party databases.[261] Allowing a company to analyze one's DNA for medical or ancestry purposes does not do away with the protection all Americans have to be free from unreasonable and unwarranted government intrusion.

Hillary L. Kody[*]

256. *See supra* Parts II.A. and II.C.
257. *See supra* notes 88-103 and accompanying text.
258. *See supra* Part III.A.
259. *See supra* Part III.A.
260. *See supra* Part III.C.
261. *See supra* Part IV.

* J.D. Candidate, 2020, William & Mary Law School; B.F.A., Writing, Literature, & Publishing, 2013, Emerson College. Thank you to Professor Paul Marcus for his helpful feedback, and Tessa Tilton for her support and thoughtful comments throughout the writing process. Thank you to the *Law Review* staff for their hard work editing this Note and Volume.