Hastings Science and Technology Law Journal

Volume 10
Number 2 *Summer 2019*

Article 2

Summer 2019

Can a Distant Relative Allow the Government Access to Your DNA? The Fourth Amendment Implications of Law Enforcement's Genealogical Search for the Golden State Killer and Other Genetic Genealogy Investigations

George M. Dery III

Can a Distant Relative Allow the Government Access to Your DNA?

The Fourth Amendment Implications of Law Enforcement's Genealogical Search for the Golden State Killer and Other Genetic Genealogy Investigations

by GEORGE M. DERY III

Abstract

This Article considers the advent of genetic genealogy, used by law enforcement in capturing the Golden State Killer suspect and in other cold cases. In these investigations, police used genetic information obtained from the open source genealogy site, GEDmatch, to build vast family trees spanning the entire country and several generations in order to locate suspects whose DNA matched that left at a crime scene. This Article analyzes the Fourth Amendment implications of government use of such powerful technology to explore such sensitive information as DNA. The conclusion the Supreme Court could reach, should it be called upon to examine the privacy issues involved in such intrusions, would vary depending on which avenue of Fourth Amendment analysis it chose to pursue. *Maryland v. King*, Court precedent on government collection of DNA, is so narrow that it provides little guidance on the issues presented by genetic genealogy. Instead, the Court could consult its recent ruling in *Carpenter v. United States*, which limited the third party doctrine that had previously nullified privacy expectations in shared information. If it relied on *Carpenter*, the Court would likely prohibit government downloads from genealogy sites without a warrant. Further, the Court could view individuals' uploads of genetic information onto open source genealogy sites as amounting to consent to view the DNA shared with all relatives. The Court might therefore apply its third party consent precedent, which, in relying on widely shared societal expectations, would likely prevent warrantless collection of genetic information from genealogy sites. The Court could, however, view police visits to genealogy sites as government searches that occurred after private intrusions. If the Court chose this approach, it could rule that law enforcement is free to collect the DNA

information because it is only viewing information already exposed by private parties. Finally, the Court could see law enforcement's use of genetic genealogy as an issue of standing, as recently analyzed in Byrd v. United States. Application of Byrd's property rights definition of standing would likely enable the government to admit genetic evidence since suspects lack the power to exclude others from open source sites. Thus, although some Fourth Amendment doctrines would forbid warrantless collection of DNA information, the government could likely rely on either antecedent private search or standing precedent to successfully use genetic genealogy evidence.

Introduction

How well do you know your relatives? Can you name every cousin, uncle, or great grandparent? Would you base your right to privacy on the whims of every one of your blood relations? Perhaps there is a "black sheep" in your family who continually runs afoul of the law. Maybe there is a flaky uncle always looking for shortcuts or a grandchild who suffers from drug addiction. Moreover, there are likely many distant relatives whose very existence is unknown to you. Would you risk the privacy of your most personal information, housed in your deoxyribonucleic acid (DNA), on this person's judgment?

On National DNA Day, Sacramento District Attorney Anne Marie Schubert announced the arrest of Joseph James DeAngelo, alleging he was the Golden State Killer,[1] believed responsible for 12 killings, 50 rapes, and 100 burglaries from 1974 and 1986.[2] To catch their quarry, police used crime scene DNA to make a partial match with the "DNA of a relative on the open-source genealogy website GEDmatch."[3] Officials then painstakingly constructed "25 family trees containing thousands of relatives" in order to trace "the killer's great-great-great grandparents, who lived in the early 1800's."[4] Investigators dug through "census records, newspaper obituaries, gravesite locators, and police and commercial databases" to whittle the possible suspects down to DeAngelo.[5] District Attorney Schubert accurately characterized law enforcement's efforts as

1. Ray Sanchez, Elizabeth I. Johnson, Steve Almasy & Alanne Orjoux, *After Searching for more than 40 Years, Authorities Say an Ex-cop Is the Golden State Killer*, CNN (Apr. 27, 2018, 10:44 AM), https://www.cnn.com/2018/04/25/us/golden-state-killer-development/index.html.

2. Justin Jouvenal, *To Find Alleged Golden State Killer, Investigators First Found His Great-great-great Grandparents*, WASH. POST (Apr. 30, 2018), https://www.washingtonpost.com/local/public-safety/to-find-alleged-golden-state-killer-investigators-first-found-his-great-great-great-grandparents/2018/04/30/3c865fe7-dfcc-4a0e-b6b2-0bec548d501f_story.html?utm_term=.26202e9e14a4.

3. Sarah Zhang, *How a Genealogy Website Led to the Alleged Golden State Killer: Powerful Tools are Now Available to Anyone Who Wants to Look for a DNA Match, Which Has Troubling Privacy Implications*, THE ATLANTIC (Apr. 27, 2018), https://www.theatlantic.com/science/archive/2018/04/golden-state-killer-east-area-rapist-dna-genealogy/559070/.

4. Jouvenal, *supra* note 2.

5. *Id.*

finding "the needle in the haystack."[6] "The answer was always going to be in the DNA,"[7] she concluded.

Law enforcement have every reason to be satisfied with its apparent success in capturing the "clever" and "sadistic" criminal[8] variously known as the "East Area Rapist," the "Original Night Stalker," the "Golden State Killer,"[9] the "Diamond Knot Killer," and the "Visalia Ransacker."[10] Erika Hutchcraft, an investigator with the Orange County District Attorney's Office, considered the Golden State Killer's "[v]ery cold, very violent" crimes to be "some of the most horrific [she's] had to investigate."[11] Sacramento County Sheriff's Department Detective Carol Daly deemed this criminal "the most heinous rapist I had ever known."[12] The killer "planned meticulously," calling victims to learn their routines,[13] casing homes, cutting phone lines, and even turning off air conditioners "so he could hear every sound."[14] Such careful planning enabled his attacks to be "bizarre, cruel, and long-lasting."[15] When he was once "cornered" in a backyard with police dogs swarming the area, "he just disappeared into thin air."[16] Police, in finally capturing such a dangerous and elusive suspect, can rightly celebrate the innovation and dedication leading to such a significant achievement. Moreover, law enforcement can report other recent successes in cases long unsolved; the genetic genealogy employed in the Golden State Killer case has already been used to bring other notorious suspects to justice.[17]

6. Sanchez et al., *supra* note 1.

7. Aja Romano, *DNA Profiles from Ancestry Websites Helped Identify the Golden State Killer Suspect: He Wasn't the First Criminal to Fall to Familial DNA Matching, and He Won't Be the Last*, VOX (Apr. 27, 2018, 5:20 PM), https://www.vox.com/2018/4/27/17290288/golden-state-killer-joseph-james-deangelo-dna-profile-match.

8. Jouvenal, *supra* note 2.

9. Zhang, *supra* note 3.

10. Jouvenal, *supra* note 2.

11. Sanchez et al., *supra* note 1.

12. Jouvenal, *supra* note 2.

13. *Id*.

14. Joseph Serna, Richard Winton & Sarah Parvini, *As a Young Cop, Golden State Killer Suspect Was Aloof, Ambitious, 'Always Serious,'* L.A. TIMES (May 1, 2018, 3:00 AM), http://www.latimes.com/local/lanow/la-me-golden-state-cops-20180501-story.html.

15. Jouvenal, *supra* note 2.

16. Serna et al., *supra* note 14.

17. Kyle Swenson, *Undercover Cops Grabbed a DJ's Chewing Gum. It Helped Crack a Teacher's 1992 Murder, Police Say*, WASH. POST (June 26, 2018), https://www.washingtonpost.com/news/morning-mix/wp/2018/06/26/undercover-cops-grabbed-a-djs-chewing-gum-it-helped-crack-a-teachers-1992-murder-police-say/?utm_ter

While the stakes in tracking down the Golden State Killer and other cold-case suspects are particularly high, the Fourth Amendment privacy concerns involved in government exploration of DNA websites are equally significant.[18] DNA, after all, is the genetic blueprint of our bodies that is embedded in the nucleus—the core—of each cell in the human body.[19] The genetic material in every cell "carries the full sequence of your DNA, including the mutation pattern that makes it uniquely yours."[20] DNA holds the secret to such personal details as one's Neanderthal ancestry, the potential for afflictions with rare diseases, and paternity.[21] One expert warns, "[f]or a non-trivial percentage of us, there really are scary things in our genomes."[22] In certain circumstances, DNA is coveted by companies, insurers and police and can be considered "the most valuable thing you own."[23]

The analytical approach the Court chooses to examine government exploration of DNA on genealogical sites will determine how it decides the Fourth Amendment issues triggered by this new intrusion. Therefore, after Part II reviews the definition of a Fourth Amendment "search" and the Court's warrant requirement. Part III examines the Golden State Killer investigation, and Part IV analyzes the paths the Court might take in deciding the Fourth Amendment issues concerning genetic genealogy. Part IV discusses *Maryland v. King*'s Fourth Amendment consideration of government DNA collection,[24] and the Court's third party doctrine, which has traditionally limited the privacy expectations of those who share

m=.7abdb34dabac; *April Tinsley: DNA Snares Man in Indiana Girl's 1988 Murder*, BBC NEWS (July 16, 2018), https://www.bbc.com/news/world-us-canada-44851825.

18. The Fourth Amendment provides:

> 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.

19. Maryland v. King, 569 U.S. 435, 442 (2013).

20. Maggie Fox, *What You're Giving Away with Those Home DNA Tests: It's the Most Valuable Thing You Own*, NBC NEWS (Nov. 29, 2017, 6:46 AM), https://www.nbcnews.com/health/health-news/what-you-re-giving-away-those-home-dna-tests-n824776.

21. *Id.*; *see also* Patrick Cain, *Privacy Risks Lurk in DNA Tests, Experts Warn*, GLOBAL NEWS (Aug. 15, 2016, 7:00 AM), https://globalnews.ca/news/2879276/privacy-risks-lurk-in-dna-tests-experts-warn/.

22. Fox, *supra* note 20.

23. *Id.*; *see also* Cain, *supra* note 21.

24. Maryland v. King, 569 U.S. 435 (2013).

information. In addition, this section considers *Carpenter's* latest word on the third party doctrine, and its potential, dramatic effect on the Fourth Amendment privacy of the relatives of those who upload information to genealogy sites.[25] It then explores third party consent based on an assumption of risk and shared social expectations, and its potential impact on the official use of genealogical sites. The Court could approach government genetic genealogy as a state intrusion that occurs only after a private search has been performed, thus, triggering precedent that assesses an official probe by reference to the scope of an earlier private invasion. Finally, since the Court might question whether a person could even claim a Fourth Amendment violation from government exploration of a relative's DNA, this article explores whether a suspect could have "standing" or the right to contest an official visit to a particular genealogy site. The standing discussion will consider the Court's most recent case on this issue, *Byrd v. United States*.[26]

The Fundamentals of Fourth Amendment Protection Against Unreasonable Searches

A. The Definition of a "Fourth Amendment Search"

The Fourth Amendment prohibits "unreasonable searches and seizures" of individuals' "persons, houses, papers, and effects."[27] In *Katz v. United States*, the Court defined a "search" as a government intrusion on a person's reasonable expectation of privacy.[28] In *Katz*, the Federal Bureau of Investigation (FBI) caught Katz "transmitting wagering information by telephone from Los Angeles to Miami and Boston in violation of a federal

25. Carpenter v. United States, 138 S. Ct. 2206 (2018).

26. Byrd v. United States, 138 S. Ct. 1518 (2018).

27. U.S. CONST. amend. IV.

28. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The Court has defined "searches" in two ways: (1) as a government intrusion on a person's reasonable expectation of privacy as defined in *Katz*, and (2) as a physical occupation of private property for purposes of gaining information as defined in *United States v. Jones*, 565 U.S. 400, 404–05 (2012). *Jones* explained, "The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." *Id.* As there is no evidence in the Golden State Killer case that government officials physically visited genealogical organizations to collect information, *Jones'* physical occupation test is beyond the scope of this article. For the same reason, the analysis of Fourth Amendment "seizures" is beyond the scope of this article.

statute."[29] The FBI had obtained Katz's side of a telephone conversation by bugging his phone booth.[30] When the parties argued over whether the government's eavesdropping by an electronic device attached to the outside of the phone booth[31] constituted a "physical penetration of a constitutionally protected area," the Court rejected this formulation of the issue as "misleading."[32] The focus on "whether or not a given 'area,' viewed in the abstract, is 'constitutionally protected'" deflected attention away from the question of whether a person sought to preserve privacy, even in a publicly accessible area.[33] *Katz* concluded that a person who occupies a phone booth, "shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world." It fell to Justice Harlan, in his concurring opinion, to provide the definition of a Fourth Amendment "search:"

My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable."[34]

The Court has repeatedly employed *Katz's* definition of a search, as crafted by Justice Harlan, for five decades to determine whether searches have occurred in such diverse situations as government entry into burned buildings,[35] barns,[36] bookstores,[37] and bus bins.[38] The resulting importance of *Katz* can be seen in the fact that the Court has deemed this definition of a search its "lodestar."[39]

29. *Katz*, 389 U.S. at 348.
30. *Id*.
31. *Id*.
32. *Id*. at 350–51.
33. *Id*. at 351.
34. *Id*. at 361 (Harlan, J., concurring).
35. Michigan v. Clifford, 464 U.S. 287, 292 (1984).
36. United States v. Dunn, 480 U.S. 294, 298 (1987).
37. Maryland v. Macon, 472 U.S. 463, 469 (1985).
38. Bond v. United States, 529 U.S. 334, 338-39 (2000).
39. Smith v. Maryland, 442 U.S. 735, 739 (1979).

B. The Warrant Requirement

The Fourth Amendment prohibits all but reasonable searches and seizures.[40] Although reasonableness is "the ultimate touchstone of the Fourth Amendment," the Constitution itself provides no yardstick for measuring what is and is not reasonable.[41] The Court worried that simply deeming an official intrusion "reasonable," without tying this conclusion to "some criterion of reason," would cause protection under the Fourth Amendment to "approach the evaporation point."[42] The Court also noted that the Fourth Amendment "was in large part a reaction to the general warrants and warrantless searches that had so alienated the colonists and had helped speed the movement for independence."[43] The Framers included the "no Warrants shall issue, but upon probable cause" provision to ensure that an objective magistrate "might weigh the need to invade that privacy in order to enforce the law."[44] The Court, therefore, recognized what came to be known as the warrant requirement, which generally mandated officers obtain a warrant before making a search.[45]

Riley v. California reaffirmed the Court's warrant requirement. In *Riley*, officers accessed information on a cell phone and a smart phone.[46] The Court in *Riley* refused to allow a search of these phones as part of a search incident to arrest, instead flatly ruling, "get a warrant."[47] *Riley* explained, "[w]here a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, . . . reasonableness generally requires the obtaining of a judicial warrant."[48] If police fails to obtain a warrant, the search is presumed unreasonable unless "it falls within a specific exception to the warrant requirement."[49]

Carpenter v. United States, decided in 2018, repeatedly referenced the warrant requirement.[50] The Court noted, "our cases establish that

40. In a pertinent part, the Fourth Amendment provides, "The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated." U.S. CONST. amend. IV.

41. Riley v. California, 134 S. Ct. 2473, 2482 (2014).

42. Chimel v. California, 395 U.S. 752, 765 (1969).

43. *Id*. at 761.

44. *Id*.

45. Kentucky v. King, 563 U.S. 452, 459 (2011).

46. *Riley*, 134 S. Ct. at 2840–41.

47. *Id*. at 2495.

48. *Id*. at 2482.

49. *Id*.

50. Carpenter v. United States, 138 S. Ct. 2206, 2221, 201 L. Ed. 2d 507 (2018).

warrantless searches are typically unreasonable where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing," and, therefore, "[i]n the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement."[51] Thus, the warrant mandate, articulated by the Court as early as 1925, still limits police discretion today.[52]

The Search for the Golden State Killer Suspect and Other Investigations

The Golden State Killer was a cold-blooded "serial predator" who elaborately planned his attacks.[53] Before "closing in for the kill," he would terrorize his victims with such strange behavior as breaking into the home to take women's underwear, making hang-up phone calls, or leaving drawings on a bedroom window "that appeared to have been written in 'bodily fluids."[54] He "stalked his victims through drainage ditches" and returned to one neighborhood so many times that its residents slept in shifts.[55] He wore a mask and blindfolded and gagged his victims.[56]

In pursuing its suspect, the investigators themselves became equally careful and inventive. Paul Holes, a cold case expert who had worked as an inspector for the Contra Costa County District Attorney, spent some seven years using "open source" genealogy websites to locate the Golden State Killer suspect.[57] Holes first used "Ysearch.org" to generate a "weak match" with a 73-year-old man in Clackamas County, Oregon.[58] The man willingly

51. *Id*. at 2213. The *Carpenter* Court reiterated, "we have held that official intrusion into (a reasonable expectation of privacy) generally qualifies as a search and requires a warrant supported by probable cause." *Id.*

52. Agnello v. United States, 269 U.S. 20, 33 (1925).

53. Avi Selk, *The Most Disturbing Parts of the 171-page Warrant for the Golden States Killer Suspect*, WASH. POST (June 2, 2018), https://www.washington post.com/news/post-nation/wp/2018/06/02/the-most-disturbing-parts-of-the-171-page-warrants-for-the-golden-state-killer-suspect/?utm_term=.d4870987d966. The search warrant affidavits for this case can be viewed at: http://www.sacda.org/files/9415/2789/1272/P_v_DeAngelo_Redacted_Search_Warrant_Final.pdf [hereinafter Search Warrant].

54. *Id*.

55. *Id*.

56. Sanchez et al., *supra* note 1.

57. Matthias Gafni, *Here's the 'Open Source' Genealogy Website that Helped Crack the Golden State Killer Case*, MERCURY NEWS (Apr. 26, 2018), https://www.mercurynews.com/2018/04/26/ancestry-23andme-deny-assisting-law-enforcement-in-east-area-rapist-case/.

58. *Id*.

provided a DNA sample, which established his innocence.[59] After this setback, Holes visited other jurisdictions that had suffered the Golden State Killer's crimes in order to obtain DNA to use at a different genealogy website, GEDmatch.[60]

GEDmatch is an "open-source genealogy website" based in Florida "that pools raw genetic profiles that people publicly share to find long-lost relatives."[61] GEDmatch differs from commercial genealogy sites such as 23andMe and Ancestry.com, which charge a fee to "millions of customers wanting detailed information on their family, lineage and ethnicity."[62] 23andMe and Ancestry.com sell testing kits that require customers to supply a tube of saliva.[63] These direct-to-consumer sites then "work very hard to protect their customers' privacy."[64] A spokesperson for 23andMe declared that it had "never given customer information to law enforcement officials," and that the company did "not share information with employers or insurance companies, ever, under any circumstance."[65]

GEDmatch does not follow the direct-to-consumer sites' model. Instead of forming a commercial and confidential relationship with consumers, it invites anyone to upload DNA profiles already generated by the commercial sites.[66] Hobbyists researching their genealogy have uploaded "roughly a million distinct DNA sets" onto GEDmatch.[67] The

59. *Id*.

60. *Id*.; Richard Winton, Tracey Lien, Paige St. John & Benjamin Oreskes, *The First Step in Finding Golden State Killer Suspect: Finding His Great-great-great-grandparents on Genealogy Site*, L.A. TIMES (Apr. 27, 2018), http://www.latimes.com/local/lanow/la-me-golden-state-dna-match-20180427-story.html.

61. Gafni, *supra* note 57.

62. Justin Jouvenal, Mark Berman, Drew Harwell & Tom Jackman, *Data on a Genealogy Site Led Police to the 'Golden State Killer' Suspect. Now Others Worry About a 'Treasure Trove of Data,'* WASH. POST (Apr. 27, 2018), https://www.washingtonpost.com/news/post-nation/wp/2018/04/27/data-on-a-genealogy-site-led-police-to-the-golden-state-killer-suspect-now-others-worry-about-a-treasure-trove-of-data/?utm_term=.ff16e1d38bab.

63. Zhang, *supra* note 3.

64. Emily Shapiro, *What to Know About the Privacy of Your DNA in Wake of 'Golden State Killer' Suspect's Arrest*, ABC NEWS (Apr. 30, 2018), https://abcnews.go.com/US/privacy-dna-wake-golden-state-killer-suspects-arrest/story?id=54777919.

65. *Id*.

66. Gina Kolata & Heather Murphy, *The Golden State Killer Is Tracked Through a Thicket of DNA, and Experts Shudder*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/27/health/dna-privacy-golden-state-killer-genealogy.html.

67. Jouvenal et al., *supra* note 62. In contrast, "23andMe has more than 5 million customers, and Ancestry.com has 10 million." Kolata, *supra* note 66.

very utility of GEDmatch is based on its openness.[68] When he later learned of the government use of GEDmatch, Curtis Rogers, a GEDmatch operator noted "it has always been GEDmatch's policy to inform users that the database could be used for other uses, as set forth in the Site Policy."[69] Rogers warned, "[W]hile the database was created for genealogical research, it is important that GEDmatch participants understand the possible uses of their DNA, including identification of relatives that have committed crimes or were victims of crimes."[70] According to Paul Holes, such openness offered law enforcement officials access to "a large pool of profiles and didn't require a court order."[71]

After Holes' prompting, Steve Rhods, an investigator with the Ventura County District Attorney's Office, found a second rape kit in the county's coroner's office that proved to be "the mother lode of DNA."[72] The upload to GEDmatch revealed a distant match that was "roughly the equivalent of third cousins."[73] Holes traced back these distant relatives to find a common ancestor.[74] His search created a family lineage that "went back to 'great-great-great-grandparents in the early 1800s'" that mostly identified persons "from the East Coast or Midwest."[75] The investigators slowly tracked their suspect through the generations by tracing "offspring to the present day."[76] Holes whittled down the "huge" family trees he had created on Ancestry.com by consulting "census data, old newspaper clippings," gravesite locator, and LexisNexis.[77] The task investigators faced was daunting; out of some 25 family trees, the one including DeAngelo contained about 1,000 members.[78]

68. Gafni, *supra* note 57.

69. *Id*.

70. *Id*.

71. Ailsa Chang & Adhiti Bandlamudi, *Tactics Used To Find Golden State Killer Raise Privacy and Legal Questions*, NATIONAL PUBLIC RADIO (Apr. 27, 2018), https://www.npr.org/2018/04/27/606580162/tactics-used-to-find-golden-state-killer-raise-privacy-and-legal-questions.

72. Winton, *supra* note 60. The discovery of this DNA sample was due to the diligence of a "meticulous pathologist" who had put "a duplicate evidence kit" in a freezer in 1980. Jouvenal, *supra* note 2. "Many other DNA samples from the case had been depleted over the years." *Id*.

73. Jouvenal, *supra* note 2.

74. *Id*.

75. Winton, *supra* note 60.

76. *Id*.; Jouvenal, *supra* note 2.

77. Jouvenal, *supra* note 2.

78. *Id*.

Towards the end of the investigation, Holes had focused on five white men, including DeAngelo.[79] Holes considered some of DeAngelo's factors, such as his age and his "serving full-time as a cop," as "strike(s) against" being the killer.[80] One fact, however, was particularly damning for DeAngelo. During a July 1978 rape, the East Area Rapist "was sobbing and saying, 'I hate you Bonnie, I hate you Bonnie."[81] Investigators learned that DeAngelo "had been engaged to a woman named Bonnie in 1970."[82] In April 2018, police observed DeAngelo speeding his motorcycle down the freeway in excess of 100 miles an hour.[83] Holes noted "stop signs are optional for this guy."[84] Detectives collected DeAngelo's DNA from the door of his car while he shopped in a Hobby Lobby in Roseville, California.[85] This DNA "matched semen recovered at the scene of some of the Golden State Killer's crime scenes."[86] They later obtained a second sample "from a tissue in DeAngelo's trash outside of his home."[87] Police arrested DeAngelo on April 24, 2018.[88] The warrant police obtained to search DeAngelo's home was based in part on the earlier genealogical search in this case.[89]

The pursuit of the Golden State Killer through genealogical sites is not an isolated case. In June of 2018, Lancaster County District Attorney, Craig Stedman, announced at a news conference the arrest of Raymond Rowe for the beating, sexual assault, and strangulation of Christy Mirack.[90] Mirack was a 25-year-old schoolteacher whose murder case went cold despite the forensic testing of 60 suspects and the conducting of over 1,500

79. Ryan Lillis, *Here's the Inside Story of How Police Nabbed the East Area Rapist Suspect*, SACRAMENTO BEE (Apr. 29, 2018), http://www.sacbee.com/news/local/crime/article210003114.html.

80. *Id*.

81. *Id*.

82. *Id*.

83. *Id*.

84. *Id*.

85. Paige St. John et al., *DNA Lifted From Golden State Killer Suspect at Hobby Lobby Parking Lot Key to Cracking Case, Documents Show*, L.A. TIMES (June 1, 2018), http://www.latimes.com/local/lanow/la-me-ln-golden-state-killer-deangelo-warrant-20180601-story.html.

86. *Id*.

87. *Id*.

88. *Id*.

89. Search Warrant, *supra* note 53, at 42.

90. Swenson, *supra* note 17.

interviews.[91] Mirack's mother made a "deathbed plea in the newspaper for new information" and her brother put up a billboard and started a Facebook page seeking tips.[92] Recognizing that they "didn't have any more arrows in the quiver," authorities turned to genetic genealogy.[93] The District Attorney's Office worked with Parabon NanoLabs, which created "a genotype file" from semen found on the "carpeting under the victim's body and on her person."[94] Parabon NanoLabs uploaded this file to GEDmatch, which enabled them to build family trees offering "highly scientific" suggestions for traditional police investigations.[95] Pennsylvania State Police narrowed the search to Rowe, who was scheduled to perform as a DJ at an elementary school event.[96] Undercover officers then collected chewing gum and a water bottle that Rowe had used and then discarded.[97] The crime lab linked Rowe to the Mirack homicide with a "1 in 200 octillion chance the match is to another member of the Caucasian population who is not Rowe."[98]

Law enforcement also visited public genealogy sites to solve the 1988 abduction, rape, and strangulation-murder of eight-year-old April Tinsley of Fort Wayne, Indiana.[99] The case became Indiana's "most notorious cold case" in part due to the alleged killer's threats toward other little girls in Fort Wayne starting in 2004.[100] The attacker left notes, found inside bags with used condoms or Polaroid pictures of his body, on the girls' bicycles.[101] One note chillingly read, "Hi honey I been watching you I am the same person that kidnapped an rape an kill Aproil Tinsley you are my

91. *Id*.

92. *Id*.

93. *Id*.

94. *Id*.

95. *Id*.

96. *Id*.

97. *Id*.

98. *Id*. Investigators have also used forensic genealogy to identify victims of crime. Margaret Press and Colleen Fitzpatrick, co-founders of the DNA Doe Project, gave a name to a victim of a 37-year-old homicide case in four hours. Seth Augenstein, *Buck Skin Girl Case Break Is Success of New DNA Doe Project*, FORENSIC MAGAZINE (Apr. 16, 2018), https://www.forensicmag.com/news/2018/04/buck-skin-girl-case-break-success-new-dna-doe-project. In this case, which also relied on GEDmatch, Detective Steve Hickey of the Miami County Sheriff's Department stated this development created "an active homicide investigation." *Id*.

99. April Tinsley: DNA Snares Man in Indiana Girl's 1988 Murder, *supra* note 17.

100. *Id*.

101. *Id*.

next vitem (sic)."[102] Authorities again turned to Parabon NanoLabs to analyze the DNA samples and then visited genealogy sites to gain a list of suspects.[103] After narrowing their search to two brothers, police collected used condoms from the trash outside the trailer home of John D. Miller. Obtaining a match with the crime scene samples, officials contacted Miller and asked, "[W]hy he thought police were interested in speaking with him."[104] Police reported that Miller answered, "April Tinsley."[105]

The genetic genealogy investigations of DeAngelo, Rowe, and Miller are the advent of a potentially game-changing technology that represents hope for victims and families long suffering from seemingly unsolvable crimes. At the same time, this search technology is so uniquely powerful that it presents issues of crucial concern for Fourth Amendment rights.

Implications of the Collection and Use of DNA Information from Genealogy Sites

A. *Maryland v. King*'s Ruling on Government DNA Collection Is So Narrow that it Provides Inadequate Guidance for Government Use of Genealogy Sites

Should the Golden State Killer case reach the Court, one might suppose that the Court would consult its first case involving the Fourth Amendment implications of government use of DNA evidence in a criminal matter, Maryland v. King.[106] Close scrutiny of King, however, might not support such an assumption. In King, the Court considered "whether the Fourth Amendment prohibits the collection and analysis of a DNA sample from persons arrested, but not yet convicted, on felony charges."[107] Officers arrested Alonzo King for assault by "menacing a group of people with a shotgun."[108] Police collected a DNA sample from King, as "part of a routine booking procedure for serious offenses," by rubbing a "filter paper or cotton swab" against the inside of his cheek.[109]

102. *Id*.
103. *Id*.
104. *Id*.
105. *Id*.
106. *King*, 569 U.S. at 442.
107. *Id*.
108. *Id*. at 439.
109. *Id*. at 440, 444.

King's DNA matched a sample of DNA taken from a rape occurring six years earlier, resulting in his trial and conviction of rape.[110]

The corrections officers at the booking facility in King automatically collected DNA in reliance on a Maryland statute authorizing "law enforcement authorities to collect DNA samples from 'an 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.'"[111] The collected sample was not to be added to a government database until after probable cause was found at the arraignment or the detainee provided consent.[112] The statute specifically limited the use of DNA records to identification purposes only.[113] Maryland's law explicitly prohibited searching for "familial matches," providing: "A person may not perform a search of the statewide DNA data base for the purpose of identification of an offender in connection with a crime for which the offender may be a biological relative of the individual from whom the DNA sample was acquired."[114] Government officials uploaded King's DNA information to Maryland's DNA database.[115] The identification of King as a rapist was based in part on the "national project to standardize collection and storage of DNA profiles" known as the "Combined DNA Index System (CODIS)."[116] Created by Congress and supervised by the FBI, CODIS "has grown to include all 50 states and a number of federal agencies."[117] CODIS "collects DNA profiles provided by local laboratories taken from arrestees, convicted offenders, and forensic evidence found at crime scenes."[118]

The *King* Court concluded that routine collection and analysis of DNA upon booking was reasonable under the Fourth Amendment because "[W]hen officers make an arrest supported by probable cause to hold for a serious offense and they bring the suspect to the station to be detained in custody, taking and analyzing a cheek swab of the arrestee's DNA is, like fingerprinting and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment."[119] *King* reached this

110. *Id*. at 440.
111. *Id*. at 441, 443.
112. *Id*. at 443.
113. *Id*. at 444.
114. *Id*.
115. *Id*. at 441.
116. *Id*. at 444.
117. *Id*. at 444–45.
118. *Id*. at 445.
119. *Id*. at 465–66.

result without relying on the Fourth Amendment's traditional norms of the warrant requirement or individualized suspicion.[120] Instead, the Court assessed the reasonableness of the DNA collection by balancing the interests of government and individual.[121] To *King*, context was key; the particular circumstances in which officials assumed responsibility over persons taken into their custody both heightened government interests[122] and lessened individual privacy concerns.[123]

When considering government concerns, *King* was acutely aware of the high stakes involved in taking a person into custody because "the law is in the act of subjecting the body of the accused to its physical dominion."[124] Officials had practical reasons for knowing "who has been arrested and who is being tried."[125] Learning identity revealed criminal history, which is crucial information because persons "detained for minor offenses can turn out to be the most devious and dangerous criminals."[126] Proper identification could alert officials to "a record of violence or mental disorder," and therefore disclose "the type of person" officers are detaining."[127] Corrections officers could thus ensure that an arrestee did "not create inordinate 'risks for facility staff, for the existing detainee population, and for a new detainee.'"[128] DNA identification also promoted the "substantial interest in ensuring that persons accused of crimes are available for trials" because it alerted officials to persons likely to fail to appear in court due to outstanding pending cases.[129] Further, knowing a detainee's past was "essential to an assessment of the danger he poses to

120. *Id*. at 447.

121. The Court explained, "[W]e balance the privacy-related and law enforcement-related concerns to determine if the intrusion was reasonable." *Id*. at 448. *King* also noted, "This application of 'traditional standards of reasonableness' requires a court to weigh 'the promotion of legitimate governmental interests' against 'the degree to which [the search] intrudes upon an individual's privacy.'" *Id.* at 448.

122. *Id*. at 449–456. *King* concluded, "In the balance of reasonableness required by the Fourth Amendment, therefore, the Court must give great weight both to the significant government interest at stake in the identification of arrestees and to the unmatched potential of DNA identification to serve that interest." *Id.* at 461.

123. *Id*. at 461-464. *King* ruled, "The expectations of privacy of an individual taken into police custody "necessarily [are] of a diminished scope." *Id*. at 462.

124. *Id*. at 449–50.

125. *Id*. at 450.

126. *Id*.

127. *Id*. at 452.

128. *Id*.

129. *Id*. at 452–53.

the public," a vital factor in assessing bail eligibility.[130] Fixing identity also served "the interests of justice" because properly connecting an arrestee to a crime could exonerate someone "wrongfully imprisoned for the same offense."[131]

An individual arrestee's interests suffered by comparison to the "substantial government interest" in the "unique effectiveness of DNA identification."[132] *King* viewed the intrusion of a DNA cheek swab as "minimal"[133] and the processing of a DNA sample in CODIS as reasonable.[134] While noting that genes, "the coding regions" of DNA, provide instructions for making the proteins in an individual's body,[135] *King* dismissed the "noncoding" DNA, which the government used to make a DNA identification of a person, as "'junk' DNA"[136] which did not reveal "information beyond identification."[137]

Further, the legitimacy of privacy expectations was dependent upon "the individual's legal relationship with the State."[138] King's expectations were necessarily "diminished" because he was "an individual taken into police custody."[139] As a person who "has been arrested on probable cause for a dangerous offense," King's "freedom from police scrutiny" was simply reduced.[140] Indeed, situational factors were so central to the analysis that the Court explicitly distinguished King's DNA collection from a

130. *Id*. at 453.

131. *Id*. at 455.

132. *Id*. at 461.

133. *Id. King* described a buccal swab DNA sample as a "gentle rub along the inside of the cheek" that "does not break the skin." *Id.* at 463–64. The sample involved "virtually no risk, trauma, or pain." *Id.*

134. *Id.* at 464.

135. *Id*.

136. *Id.* at 442-43.

137. *Id.* at 464. Unfortunately, this information was outdated when the Court made its ruling, for scientists already knew even before the *King* opinion that "[S]pecific DNA once dismissed as junk plays an important role in brain development and might be involved in several devastating neurological diseases." Jeffrey Norris, *Brain Development Is Guided by Junk DNA that Isn't Really Junk*, UCSF (Apr. 15, 2013), https://www.ucsf. edu/news/2013/04/105126/brain-development-guided-junk-dna-isn%E2%80%99t-really-junk. While the Norris article is dated April 15, 2013, the Court decided *King* on June 3, 2013. Any information of a genetic predisposition for a "devastating" neurological disease, in light of the possible consequences for such practical matters as insurance and employment, could rightly be seen as highly personal and sensitive.

138. *King*, 569 U.S. at 462.

139. *Id*.

140. *Id.* at 463.

search of "the average citizen."[141] *King* warned that changing context could result in a different ruling; the Court noted, "If in the future police analyze samples to determine, for instance, an arrestee's predisposition for a particular disease or other hereditary factors not relevant to identity, that case would present additional privacy concerns not present here."[142] The Court thus concluded, "In light of the context of a valid arrest supported by probable cause respondent's expectations of privacy were not offended" by the DNA collection in this case.[143]

As the Court's only case directly dealing with a Fourth Amendment search of a person's DNA, *King* must be accounted for when considering police use of genetic genealogy. *King* deemed reasonable the mandatory collection of DNA from arrestees of violent offenses about to be taken into official custody.[144] The utility of this holding in assessing government collection of DNA information from genealogical sites, however, might be quite limited. The context of *King*, so important to the Court, significantly differed from that of genetic genealogy. In *King*, officers had probable cause that the person searched had committed a crime.[145] The government therefore had the "uncontested" right, "always recognized under English and American law," to search the lawfully arrested person.[146] Further, King was jailed and therefore exposed to booking procedures having "different constitutional justifications" than searches in other places.[147] *King's* jail context was crucial because State interests "are further different" when the government takes on the grave responsibility of "subjecting the body of the accused to its physical dominion."[148] In this setting, DNA identification was critical for a host of government interests, including safety of staff, fellow prisoners, and the arrestee himself,[149] determination of availability for trial, potential danger to the public,[150] and the interests of justice.[151] In contrast, the government visits to genealogy sites in pursuit of DeAngelo, Rowe, and Miller lacked all the contextual justifications bolstering *King's*

141. *Id.*
142. *Id.* at 464–65.
143. *Id.* at 465.
144. *Id.* at 465–66.
145. *Id.* at 449
146. *Id*.
147. *Id*.
148. *Id.* at 449-50.
149. *Id.* at 452.
150. *Id.* at 452-53.
151. *Id.* at 453.

collection of DNA. To say that police lacked probable cause pinpointing these suspects is an enormous understatement; law enforcement did not even have these individuals on its radar. As for jail, these cases had become so cold that, before GEDmatch, subjecting the bodies of these suspects to the government's physical dominion was a practical impossibility.

King's contextual limit similarly suffers when comparing King's individual interests with those of the genetic genealogy suspects. King, due to his "legal relationship with the state" as an arrestee entering custody, had "diminished" privacy expectations.[152] DeAngelo, Rowe, and Miller, having no such custodial relationship with the State when law enforcement visited the genealogy sites, suffered no corresponding diminution of privacy expectations. Instead, they were the very "average citizen(s)" *King* distinguished from jail inmates.[153] Finally, *King* explicitly noted its case did not involve "familial" matching," the central strategy involved in the genetic genealogy cases.[154] Thus, while *King* offers a detailed picture of the Court's analysis of Fourth Amendment privacy issues involving DNA, the narrowness of its ruling undermines its usefulness in providing guidance for government exploration of genealogical sites.

B. *Carpenter v. United States'* Recent Limit on the Third Party Doctrine, Which Held that Persons Undermine Their Privacy Expectations by Sharing Information, Could Dramatically Constrain Government Downloads from Genealogical Sites

When one uploads his or her genetic information onto a genealogical site, he or she shares it with third parties. The whole point of exposing this information to the public on the website is to enable someone else to access the information about one's DNA in hopes of identifying lost or unknown relatives. In revealing genetic information when searching for one's family, is a person giving up his or her right to privacy from a government search of this information? The Court's third party doctrine could directly affect the Fourth Amendment rights of those who upload their DNA.[155]

Katz rejected the notion that a Fourth Amendment "search" requires a physical trespass upon a constitutionally protected area, explaining that what a person "seeks to preserve as private, even in an area accessible to

152. *Id.* at 462.

153. *Id.* at 463.

154. *Id.* at 441.

155. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

the public, may be constitutionally protected.[156] By the same token, however, the Court declared, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[157] *Katz*'s "knowingly exposes" language ultimately took on great significance in creating the third party doctrine where "an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[158]

For decades, the Court ruled that sharing information with another person often amounted to losing any Fourth Amendment privacy protection in the information disclosed. In *United States v. Dionisio*, where a grand jury subpoenaed an illegal gambling suspect to provide a voice exemplar for comparison with FBI recordings, the Court found that the government demand involved no intrusion on a reasonable expectation of privacy.[159] Because "nothing is being exposed to the grand jury that has not previously been exposed to the public at large," Dionisio could not have "a reasonable expectation that others" would not know the sound of his voice "any more than he can reasonably expect that his face will be a mystery to the world."[160]

Information sharing with a "third party" squandered Fourth Amendment privacy in *United States v. Miller*.[161] In *Miller*, the government sought a bank depositor's "checks and other bank records" in its investigation of the depositor's unregistered still and whiskey business.[162] When Miller objected that his bank documents had been illegally seized, the Court found no intrusion of a Fourth Amendment interest.[163] *Miller* noted that the depositor, "in revealing his affairs to another," took the risk that the information so revealed would "be conveyed by that person to the Government."[164] The Court therefore ruled, "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose

156. *Id.* at 351.
157. *Id*.
158. *Jones*, 565 U.S. at 417.
159. United States v. Dionisio, 410 U.S. 1, 13-14 (1973).
160. *Id.* at 14.
161. United States v. Miller, 425 U.S. 435, 444 (1976).
162. *Id*. at 436.
163. *Id.* at 438, 440.
164. *Id.* at 443.

and the confidence placed in the third party will not be betrayed."[165] Sharing information, even as sensitive as personal finances and even with an institution as discrete as a bank, led to exposure of that information to the government without Fourth Amendment protection.

In *Smith v. Maryland*, the Court determined that what was true about sharing one's voice and banking records was also true about sharing numbers dialed from a phone.[166] In *Smith*, police used a pen register to collect the numbers a robber dialed from his phone in making threatening calls to a robbery victim.[167] When Smith sought to suppress the dialed numbers, the Court refused to do so, noting that he "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business"[168] *Smith* declared once again that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[169]

The Court, in *California v. Greenwood*, even applied its third party doctrine to persons who roll their trash to the curb for collection.[170] *Greenwood* found no Fourth Amendment search occurred when police rummaged through garbage for narcotics evidence because the residents "exposed their garbage to the public sufficiently to defeat their claim to Fourth Amendment protection."[171] Placing trash on the curb made it "readily accessible to animals, children, scavengers, (and) snoops."[172] The whole point of leaving refuse at the curb was "for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through respondents' trash or permitted others, such as the police, to do so."[173] Therefore, there was "no reasonable expectation of privacy" in the discarded items.[174]

The Court's latest pronouncement on the third party doctrine, in its 2018 case, *Carpenter v. United States*, was more nuanced than previous declarations. In *Carpenter*, police officers and FBI agents suspected Timothy Carpenter of being involved in robberies of nine stores in

165. *Id.*
166. Smith v. Maryland, 442 U.S. 735 (1979).
167. *Id.* at 742.
168. *Id.* at 737, 744.
169. *Id.* at 743–44.
170. California v. Greenwood, 486 U.S. 35 (1988).
171. *Id.* at 37–38, 40.
172. *Id.* at 40.
173. *Id.*
174. *Id.* at 41.

Michigan and Ohio.[175] Federal prosecutors therefore sought court orders "under the Stored Communications Act" to obtain Carpenter's cell phone records.[176] Federal magistrate judges ordered MetroPCS and Sprint to provide cell site information for Carpenter's phone over the four months during which the robberies were committed.[177] Pursuant to the orders, agents collected "cell-site location information (CSLI)" over 127 days from MetroPCS alone.[178] CSLI is the information wireless carriers collect from cell phones in order to "continuously scan their environment looking for the best signal, which generally comes from the closest cell site."[179] Smartphones tap into the wireless network "several times a minute" even when the owner is not using the phone.[180] The resulting "time-stamped" records, which companies store for their own business purposes, are the CSLI.[181] CSLI gives authorities a precise map of where a phone, and therefore the phone's owner, has been. The collection of Carpenter's CSLI provided officials with "12,898 location points cataloging Carpenter's movements—an average of 101 data points per day."[182] When the government used the CSLI to place Carpenter near four of the robberies, Carpenter objected that the use of these data constituted an unreasonable search made in absence of a warrant or an exception to the warrant requirement.[183]

In considering Carpenter's claim, the Court acknowledged that it had previously held, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[184] The government, therefore, was "typically free to obtain" the shared information "from the recipient without triggering Fourth Amendment protections."[185] *Carpenter*, however, asserted that the third party doctrine had been limited from the start. The Court noted that, in *Miller*, the case

175. *Carpenter v. United States*, 138 S. Ct. 2212 (2018).

176. *Id.* The level of suspicion needed to support the court orders was "specific and articulable facts showing that there are reasonable grounds to believe." *Id.* Such reasonable suspicion falls short of the Fourth Amendment requirement of probable cause for a warrant. U.S. CONST. amend. IV.

177. *Id*.

178. *Id*.

179. *Id*. at 2211.

180. *Id*.

181. *Id*. at 2211, 2212.

182. *Id*. at 2212.

183. *Id*.

184. *Id*. at 2216.

185. *Id*.

where the third party doctrine traced its "roots," the information lacking Fourth Amendment protection had: 1) a particular "nature," and 2) a specific relationship with the person claiming privacy.[186] The nature of *Miller's* documents "confirmed Miller's limited expectation of privacy" because they were "not confidential communications but negotiable documents," such as checks "exposed" to employees "in the ordinary course of business."[187] As for Miller's relationship with the documents, it was quite weak because he could "assert neither ownership nor possession" of the papers.[188] *Carpenter* then declared that *Smith*, the third party case occurring only three years after *Miller*, was a similarly narrow case.[189] *Smith* involved pen registers—devices that merely recorded numbers dialed from a phone—a technology with "limited capabilities."[190] Together, *Miller* and *Smith* "did not rely solely on the act of sharing" but instead took into account the "nature" of the information sought and the "limited capabilities" of the government technology used to collect the information.[191]

Carpenter then distinguished *Miller* and *Smith* from the facts in its own case. The nature of the information collected in *Carpenter* represented a "world of difference" from that obtained in *Miller* and *Smith*.[192] The CSLI presented "an all-encompassing record" of the "privacies of life," including aspects of "familial, political, professional, religious, and sexual associations."[193] Unlike prior methodologies, cell phone location had a "retrospective quality" enabling the government to "travel back in time" to reconstruct a person's movements "every moment of every day for five years."[194] Further, unlike the information in earlier third-party precedent, CSLI information had a particularly intimate relationship with the phone user because a cell phone has become "almost a 'feature of human anatomy'" that can reveal visits to "doctor's offices, political headquarters, and other potentially revealing locales."[195] Finally, the capabilities of CSLI represented a "seismic shift" in technology from *Miller* and *Smith* because

186. *Id*.
187. *Id*.
188. *Id*.
189. *Id*.
190. *Id*.
191. *Id*. at 2219.
192. *Id*.
193. *Id*. at 2217.
194. *Id*. at 2218.
195. *Id*.

the "exhaustive chronicle of location information" can be "casually collected" with a "click of a button."[196]

DNA, in 1) the nature of the information it contains, 2) the relationship of that information with the individuals claiming Fourth Amendment protection and 3) the capability of the technology exploiting it, shares similarities with the CSLI in *Carpenter*. Analysis of these three factors indicates that the Court would refuse to extend its third-party doctrine to warrantless government collection of DNA information from genealogical sites. Trouble starts for officials using genetic genealogy with the first factor regarding the "nature" of the information collected. It is hard to overstate the intimacy of DNA information, housed in the "nucleus of all human cells," which offers a blueprint to the entire body.[197] DNA provides a "treasure trove" of private data, including details on "family, lineage and ethnicity" and even a window into potential disease.[198] The very sensitivity of DNA information forces commercial sites such as 23andMe to "work very hard to protect their customers' privacy."[199] While *Carpenter's* CSLI could reveal a visit to the doctor's office, DNA could expose the underlying health issue itself.[200]

Carpenter's focus on the relationship of information to the individual also favors Fourth Amendment protection of genealogical information. If a cellphone is "almost a 'feature of human anatomy,'" DNA is quite literally a feature of human anatomy.[201] DNA is "deeply revealing" precisely because it intimately maps a person's behavior and, in part, fate.[202] Without discounting the importance of environment, DNA has been linked to such deeply sensitive personal traits as promiscuity, learning ability, and violent criminality.[203] The information on genealogy sites would therefore

196. *Id*. at 2219.

197. *King*, 569 U.S. at 442.

198. Jouvenal et al., *supra* note 62.

199. Shapiro, *supra* note 64.

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

201. *Id*.

202. *Id*. at 2223.

203. Susan Donaldson James, *Thrill-Seeking Gene Can Lead to More Sex Partners*, ABC NEWS (Dec. 6, 2010), https://abcnews.go.com/Health/scientists-discover-gene-responsible-cheating-promiscuous-sex-habits/story?id=12322891 ("[A]bout half of all people have a gene that makes them more vulnerable to promiscuity and cheating."). Julia Rosen, *About Half of Kids' Learning Ability Is in Their DNA, Study Says*, L.A. TIMES (July 11, 2014), http://www.latimes.com/science/sciencenow/la-sci-sn-math-reading-genes-20140711-stor y.html ("[A]pproximately half of False children's math and reading ability stemmed from their genetic makeup."). Melissa Hogenboom, *Two Genes Linked with Violent Crime*, BBC NEWS (Oct. 28, 2014), https://www.bbc.com/news/science-enviro nment-29760212

represent a "world of difference" from *Miller* and *Smith*, thus distinguishing this precedent into insignificance.[204]

Finally, *Carpenter's* discussion regarding the capabilities of the government technology being used militates against allowing visits to genealogical sites without a warrant. *Carpenter* forbade warrantless use of cell phone data because of the "depth, breadth, and comprehensive reach" of CSLI technology.[205] The daunting scope of CSLI searches was presumably due to its ability to penetrate fully into the many aspects of its target's lives by learning a person's every location in collecting no less than 101 data points a day.[206] In comparison, the DNA making up genealogical information penetrates at a deeper level, revealing such secrets as susceptibility to certain diseases, such as breast cancer, Huntington's disease, and cystic fibrosis.[207] Moreover, DNA can reveal a person's potential longevity, risk of obesity, his or her body clock (whether an early riser or a night owl), and possession of "sensation-seeking and impulsive tendencies."[208] Therefore, the Court that was offended by the prospect of the government tracking individuals by every nearby cell site would likely be appalled by official intrusion into DNA.

Further, *Carpenter* worried about the "inescapable and automatic nature" of CSLI collection.[209] Anyone who uses a smartphone—a technology so necessary today that people "compulsively carry cellphones with them all the time"—is exposed to information collection even when the phone is not in use.[210] DNA housed on genealogy sites shares the involuntary character of CSLI exposure. No one could stop a government official from looking at the DNA one shares with a relative. Once an individual uploads his or her DNA, any distant cousin or granddaughter sharing this DNA is helpless to opt out. More fundamentally, one does not choose his or her DNA at birth and, so far, has no ability to change it

("A genetic analysis of almost 900 offenders in Finland has revealed two genes associated with violent crime.").

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

205. *Id*. at 2223.

206. *Id*. at 2212.

207. James Randerson, *What DNA Can Tell Us: Genes Alone Cannot Account for What a Person Is, But Even the Slightest Distinguishing Traits Between People Can be Attributed to Individual Genes*, THE GUARDIAN (Apr. 26, 2008), https://www.theguardian.com/science/2008/apr/27/genetics.cancer.

208. *Id*.

209. *Carpenter*, 138 S. Ct. at 2223.

210. *Id*. at 2218.

thereafter. The DNA, automatically self-replicating in each cell, generates by a process beyond human will.

Carpenter also feared the time-machine character of CSLI technology, noting that a search of cell site data enabled officials to "travel back in time to retrace a person's whereabouts.[211] To perform such tracking, police "need not even know in advance whether they want to follow a particular individual, or when."[212] When it comes to investigating the intricate details of a person's past, DNA is even more Orwellian than CSLI. While CSLI can allow the government to review "five years," genealogical genetics enables officialdom to explore untold generations.[213]

In the past, the Court has recognized the potential for "highly sophisticated" technology to corrode privacy.[214] Indeed, the Court has explicitly noted, "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."[215] *Carpenter's* concerns, therefore, are not unjustified. If the Court found CSLI collection to be "qualitatively different" from earlier cases allowing government access to shared information, the prospect of official use of the even more intrusive technology—genetic genealogy—will likely raise the Court's ire.[216] When confronted with government exploitation of genealogy sites, therefore, the Court will probably follow *Carpenter* in ensuring that the "'progress of science' does not erode Fourth Amendment protections."[217]

C. The Fourth Amendment's Third-Party Consent Precedent Will Likely Not Support Government Exploration of Genealogical Sites for Genetic Information

When a person uploads his or her DNA information to a genealogy site, this individual is giving consent for others to access this information.

211. *Id*. at 2210.

212. *Id*. at 2218.

213. *Id.*; Jouvenal, *supra* note 2. Further, certain language in *Carpenter* indicated that the Court might find the very purpose for which the government visited a genealogical site to be concerning. In downplaying the intrusiveness of Smith's pen registers, *Carpenter* noted that such "telephone call logs reveal little in the way of 'identifying information.'" *Id*. at 19. The entire purpose of examining genealogical data in the Golden State Killer case was to identify the Golden State Killer suspect—to name an individual as perpetrator.

214. Dow Chemical Co. v. United States, 476 U.S. 227, 238 (1986).

215. Kyllo v. United States, 533 U.S. 27, 33–34 (2001).

216. *Carpenter*, 138 S. Ct. at 2216.

217. *Id*. at 2223.

Since the genetic information the person is providing is partly shared by others, the upload could be seen as an example of third-party consent, where one person gives permission to intrude on an area or thing commonly possessed with another. The Court explored the Fourth Amendment implications of third-party consent in *United States v. Matlock*.[218] In *Matlock*, police officers arrested William Matlock for robbery in the front yard of his residence.[219] After placing Matlock in a squad car,[220] the officers went to the house and met Mrs. Gayle Graff, "who was dressed in a robe and was holding her son in her arms."[221] Mrs. Graff permitted police to search for money and a gun in the bedroom of a home that she jointly occupied with Matlock.[222] As a result of the consensual search of the bedroom, officers found $4,995.00 in cash inside a diaper bag.[223]

Since Matlock himself did not consent to the search, the issue before the Court was "whether Mrs. Graff's relationship to the east bedroom was sufficient to make her consent to the search valid against . . . Matlock."[224] The Court ruled, "the consent of one who possesses common authority over premises or effects is valid as against the absent, nonconsenting person with whom that authority is shared."[225] A person's "common authority" to give consent is not based on "mere property interest."[226] This power instead rests "on mutual use of the property by persons generally having joint access or control for most purposes."[227] The sharing of access or control makes it "reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched."[228] In sharing a place with another person, one automatically assumes that other person might expose that "common area"

218. United States v. Matlock, 415 U.S. 164, 170 (1974).
219. *Id*. at 166.
220. *Id*. at 179 (Douglas, J., dissenting).
221. *Id*. at 166.
222. *Id*.
223. *Id*. at 166–67.
224. *Id*. at 167.
225. *Id*. at 170.
226. *Id*. at 171, n. 7.
227. *Id*.
228. *Id*.

to others, even the police. Thus, Matlock, in sharing a bedroom with Mrs. Graff, took the risk that she might allow officers to enter and search it.[229]

Matlock, tucked away in a patrol car before police approached his home, never had the opportunity to object to a search of his bedroom.[230] Scott Randolph, in *Georgia v. Randolph*, was under no similar restraint.[231] In *Randolph*, Scott Randolph was present and arguing with his estranged wife, Janet Randolph, when she "readily gave" consent to search for Scott's "items of drug evidence" in their house.[232] Relying on Janet's consent, the officer recovered cocaine from the Randolph's bedroom.[233] The issue presented to the Court was whether a search based on third party consent is lawful "with the permission of one occupant when the other, who later seeks to suppress the evidence, is present at the scene and expressly refuses to consent."[234] *Randolph* held, "a physically present co-occupant's stated refusal to permit entry prevails, rendering the warrantless search unreasonable and invalid as to him."[235]

Randolph based its ruling on "widely shared social expectations."[236] Society's understanding about who possesses the authority to consent to a particular search, while influenced by property law, is "not controlled by its rules."[237] Instead, social expectations about consent are "a function of commonly held understandings about the authority that co-inhabitants may exercise in ways that affect each other's interests."[238] *Randolph* elucidated its "commonly held understanding" concept through a series of examples. The Court first presented the societal expectations of *Matlock*:

> When someone comes to the door of a domestic dwelling with a baby at her hip, as Mrs. Graff did, she shows that she belongs there, and that fact standing alone is enough to tell a law enforcement officer or any other visitor that if she occupies the place along with others, she probably lives there subject to the assumption tenants usually make about their common authority

229. *Id*. at 175–76.

230. *Id*. at 179 (Douglas, J., dissenting).

231. Georgia v. Randolph, 547 U.S. 103 (2006).

232. *Id*. at 107.

233. Specifically, the officer found "a section of a drinking straw with a powdery residue he suspected was cocaine." *Id.*

234. *Id*. at 106.

235. *Id*.

236. *Id*. at 111.

237. *Id*.

238. *Id*.

> when they share quarters. They understand that any one of them may admit visitors, with the consequence that a guest obnoxious to one may nevertheless be admitted in his absence by another.[239]

Matlock, in choosing to live in such an arrangement, assumed a risk that his cohabitant would invite others inside the home in his absence, an arrangement so typical that officers rightly could rely upon it without making inquiries into the possibility of some "eccentric scheme" to the contrary.[240] In contrast, *Randolph* noted that "no common authority could sensibly be suspected" for a landlord offering admission into an apartment without first seeking permission from the tenant or a hotel manager allowing entry into a room without asking for approval from the current hotel guest.[241] Moreover, an eight-year-old child, who could invite a "pollster or salesman" across the threshold of a home, could not allow rummaging "through his parents' bedroom."[242] Finally, a homeowner's authority to admit someone "over the objection of" his or her houseguest was limited because of the "customary expectation of courtesy or deference" shown a houseguest.[243] *Randolph* concluded, "there is no common understanding that one co-tenant generally has a right or authority to prevail over the express wishes of another, whether the issue is the color of the curtains or invitations to outsiders."[244]

The Court again considered a "disputed invitation"[245] in *Fernandez v. California*, a case in which Fernandez objected to an officer's entry by announcing, "You don't have any right to come in here. I know my rights."[246] Having probable cause that Fernandez had assaulted his domestic partner, police arrested him and took him to the station.[247] An officer then returned to Fernandez's residence, successfully gaining permission to search from his domestic partner, Rojas.[248] The resulting search recovered evidence linking Fernandez to a robbery.[249] While noting

239. *Id*.

240. *Id*. at 111–12.

241. *Id*. at 112 (further explaining that "a hotel guest customarily has no reason to expect the manager to allow anyone but his own employees into his room").

242. *Id*.

243. *Id*. at 113.

244. *Id*. at 114.

245. *Id*.

246. Fernandez v. California, 571 U.S. 292, 303-304 (2014).

247. *Id*.

248. *Id*.

249. *Id*. at 1131.

that a caller would have "no confidence" in one occupant's invitation if a co-occupant was present and objecting, *Fernandez* believed that the calculus "would be quite different" if "the objecting tenant was not standing at the door."[250] With the objecting occupant absent, "the friend or visitor is much more likely to accept the invitation to enter."[251] *Fernandez* thus adhered to the social norms analysis developed in *Randolph*.

If the Court applied only *Matlock's* "assumption of risk" test, it would provide inadequate answers for those whose relatives have uploaded DNA onto genealogical websites.[252] When a person shares his or her genetic information with an open source site, such as GEDmatch, this individual makes a privacy decision for his or her whole family.[253] The GEDmatch user forfeits "the genetic privacy of an entire family for generations,"[254] destroying the privacy both of relatives unknown and unborn. *Matlock's* reliance on "mutual use" would fail family members because even though two distant relatives may both possess certain segments of information in their chromosomes, such "mutual use" would fail to establish the "common authority" envisioned by the Court.[255] Rather than making a conscious choice to share a particular piece of property, relatives having the same portion of DNA instead share information—without any volitional decision. Also, unlike *Matlock's* shared bedroom, mutual use does not provide "joint control," as each relative "uses" his or her genome separately and automatically, through biological processes, without input from any other family member.[256] This lack of interaction among mutual users denies any opportunity to negotiate the terms of privacy. Since the transmission of DNA by birth is a wholly programmed process, common possessors of DNA could not be said to have "assumed the risk" that, in the involuntary "act" of sharing genes with family, any particular member has

250. *Id*. at 1135.

251. *Id*.

252. *Matlock*, 415 U.S. at 171, n. 7.

253. New York University Law Professor Erin Murphy explained, "If I'm making a decision that affects my brother, my sister, my father, my children, essentially everybody I'm related to, I think that's really different." Megan Jula, *The Breakthrough DNA Technique that Led Cops to the Golden State Killer Suspect Is Exciting—and Terrifying*, MOTHER JONES (Apr. 27, 2018), https://www.motherjones.com/crime-justice/2018/04/the-breakthrough-dna-technique-that-led-cops-to-the-golden-state-killer-suspect-is-exciting-and-terrifying/.

254. *Id*.

255. *Matlock*, 415 U.S. at 170.

256. *Id*. at 171, n. 7.

consciously chosen to allow another to expose shared information.[257] Since *Matlock's* underlying assumptions do not apply in the genetic genealogy context, its reasoning lacks convincing force, and therefore the case offers little guidance to the Court regarding government visits to genealogical sites.

In the face of *Matlock's* inadequacy in assessing genetic genealogy, the Court could turn to *Randolph* and *Fernandez*. However, as currently applied, *Randolph's* and *Fernandez's* objecting occupant would not clarify genealogical privacy issues. Considering "widely shared social expectations," *Randolph* bridled at the thought of overriding a physically present co-occupant's refusal to allow entry.[258] In contrast, *Fernandez* considered the situation "quite different" when an objecting tenant failed to be "standing at the door."[259] Since each of us has an untold number of relatives who could access genealogical sites at any time and any place on the globe, we cannot be ever-present at each computer a relative is using to access the Internet. All of us would inevitably be an absent occupant in most places and at most times. Under *Fernandez*, our absence at each genealogical site "door" upon which the government knocked when exploring DNA would deny us a right to privacy. Given the lack of an actual objection, the Court would simply return to the absent—and silent—cohabitant originally considered in *Matlock*.

To adequately address third party consent in the genetic genealogy context, the Court would need to refine *Randolph's* "widely shared social expectations" test for *Matlock's* absent and un-objecting mutual user context.[260] While *Randolph* did apply its societal expectations test to *Matlock's* facts, it concluded that an occupant could admit an "obnoxious" visitor in the cohabitant's absence.[261] Given the inability of an individual to be at every door the government might open by visiting a genealogy site, *Randolph's* willingness to admit every obnoxious visitor might be strained to the breaking point.

A flat rejection of *Randolph's* conclusion, however, would not alone identify the "widely shared social expectations" about genealogy sites.[262] There is a difficulty in analyzing social expectations in this context, due to the recent advent of genealogy sites. GEDmatch began operations as late as

257. *Id*.
258. *Randolph*, 547 U.S. at 106, 111.
259. *Fernandez*, 571 U.S. at 303.
260. *Randolph*, 547 U.S. at 111.
261. *Id*.
262. *Id*.

2010.[263] Such newness has not allowed for a full societal consensus to emerge. In contrast, the rights of the homeowner have been understood with relative certainty since 1603, when articulated in *Semayne's Case*.[264] Further, a "consensus" has not even been formed in individual minds, if one considers the inconsistent behavior of persons using the Internet. Often people will blithely give up privacy by clicking "agree" to myriad privacy policies they have chosen not to read. When privacy invasions make the news, however, these same persons can be brought up short by the intrusiveness of an incursion. Peter Neufeld of The Innocence Project has noted, "There is a whole generation that says, 'I don't really care about privacy," until "there is a Cambridge Analytica."[265] Neufeld continued, "No one has thought about what are the possible consequences."[266] This same dynamic could play out with genealogy sites. Focused on the immediate goal of tracking down a lost relative, persons might not see the long view which, had they pondered it, could appall them.

If, with the passage of time, persons did pause to consider the privacy concerns of genetic genealogy, most would likely not expect that their relatives, however distant or unknown, could permit entry into something as "deeply revealing" as DNA.[267] It is one thing to enable another person to allow exploration of the privacy of a shared home. It is quite another to permit investigation into the privacy of shared genes. Although the issue has not had time to fully cohere, "widely shared social expectations" will likely forbid one person giving the government permission to use shared DNA against a relative.

263. Cyrus Farivar, *GEDmatch, a Tiny DNA Analysis Firm, Was Key for Golden State Killer Case*, ARS TECHNICA (Apr. 27, 2018), https://arstechnica.com/tech-policy/2018/04/gedmatch-a-tiny-dna-analysis-firm-was-key-for-golden-state-killer-case/ ("In fact, when it first began in 2010, GEDmatch did not even require a login.").

264. Wilson v. Arkansas, 514 U.S. 927, 931 (1995).

265. Kolata, *supra* note 66; *see generally* Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html. ("Cambridge Analytica, a political data firm hired by President Trump's 2016 election campaign, gained access to private information on more than 50 million Facebook users. The firm offered tools that could identify the personalities of American voters and influence their behavior.")

266. Kolata, *supra* note 66.

267. *Carpenter*, 138 S. Ct. at 2223.

D. If the Court Characterizes Law Enforcement's Use of Genealogical Sites as a Government Search that Occurred after a Private Intrusion, the Lawfulness of the Official Search Will Be Assessed in Reference to the Scope of the Earlier Private Search

Suppose your neighbor, hoping to borrow a cup of sugar, enters the cupboard of your unlocked home without permission while you are away. Suppose further that your neighbor, looking in your bag of sugar, finds powder cocaine, of which he promptly tells the police. Nothing stops law enforcement from taking and using that knowledge about the cocaine's existence. Once a secret is out in the open, it can no longer be a secret; any privacy interest in that bit of information is dead.

Therefore, the Court has determined that an invasion of privacy by an individual citizen can have Fourth Amendment consequences on a later government search. In *Walter v. United States*, packages containing 871 boxes of sexually explicit 8-millimeter films were delivered to the wrong address, the hosiery company, L'Eggs Products, Inc.[268] When employees at the company opened the packages, they found on the boxes within "suggestive drawings" and "explicit descriptions of the contents."[269] They alerted the FBI to their find, causing agents to pick up the films and view them with a projector.[270] As a result, the federal government charged the defendant with interstate transportation of obscene films.[271] The *Walter* Court thus confronted the issue of "whether the Fourth Amendment required the agents to obtain a warrant before they screened the films."[272]

In considering the case, *Walter* noted that no Fourth Amendment violation occurred when the L'Eggs employees themselves opened the packages because "a wrongful search or seizure conducted by a private party does not violate the Fourth Amendment."[273] Further, the "private wrongdoing" did not "deprive the government of the right to use evidence

268. Walter v. United States, 447 U.S. 649, 651 (1980); *see also* United States v. Jacobsen, 466 U.S. 109, 115 (1984) ("While there was no single opinion of the Court [in *Walter*], a majority did agree on the appropriate analysis of a governmental search which follows on the heels of a private one.").

269. *Id*. at 651–52.

270. *Id*. at 652.

271. *Id*.

272. *Id*. at 651.

273. *Id*. at 656.

that it ha(d) acquired lawfully."[274] *Walter* measured the reasonableness of the government intrusion by reference to the earlier private invasion, noting that nothing was wrongful about the government's examination of the packages' contents "to the extent that they had already been examined by third parties."[275] Noting the evils of the "indiscriminate searches" performed under general warrants, *Walter* declared that any authorized search was "limited by the particular terms of its authorization."[276] In like manner, a private party's "invasion of another person's privacy" limited a later official search.[277] While the government could reexamine the materials previously viewed by private persons, it could not "exceed the scope" of the prior private search without independent justification.[278] Essentially, "the legality of the governmental search" had to be "tested by the scope of the antecedent private search."[279]

In *Walter*, the private search was limited, involving only the opening of the package to reveal the explicit drawings and pictures on the boxes inside, while the FBI's intrusion was more invasive, including the watching of the actual films.[280] Therefore, the earlier private search only frustrated the defendant's reasonable privacy expectations "in part;" it "did not simply strip the remaining unfrustrated portion of that expectation of all Fourth Amendment protection."[281] Ultimately, *Walter* ruled that since "the additional search conducted by the FBI—the screening of the films—was not supported by any justification," it violated the Fourth Amendment.[282]

Package problems were the focus of the Court's next private party search case, *United States. v. Jacobsen*.[283] In *Jacobsen*, Federal Express employees, pursuant to company policy regarding insurance claims, examined "an ordinary cardboard box wrapped in brown paper" that was "torn by a forklift."[284] Inside the box, employees found a 10-inch long duct-tape tube, which they opened, finding plastic bags of white powder.[285]

274. *Id*.
275. *Id*.
276. *Id*. at 657.
277. *Id*.
278. *Id*.
279. United States v. Jacobsen, 466 U.S. 109, 116 (1984).
280. *Walter*, 447 U.S. at 651–52.
281. *Id*. at 659.
282. *Id*.
283. United States v. Jacobsen, 466 U.S. 109 (1984).
284. *Id*. at 111.
285. *Id*.

Replacing the bags in the tube and the tube into the box, the employees then alerted the Drug Enforcement Administration (DEA).[286] Upon arrival the DEA agent:

> saw that one end of the tube had been slit open; he removed the four plastic bags from the tube and saw the white powder. He then opened each of the four bags and removed a trace of the white substance with a knife blade. A field test made on the spot identified the substance as cocaine.[287]

The Court in *Jacobsen* adopted the reasoning it applied in *Walter*. *Jacobsen*, noting that Federal Express employees cut the tube and exposed the white powder, declared, "Whether those invasions were accidental or deliberate, and whether they were reasonable or unreasonable, they did not violate the Fourth Amendment because of their private character."[288] The DEA's "additional invasions" had to be "tested by the degree to which they exceeded the scope of the private search."[289] If the DEA did not move beyond the private invasion, then there was no Fourth Amendment violation.[290] Since the defendant could not complain about a frustration of privacy expectations by a private party, the government was welcome to use the "now-nonprivate information."[291] If instead the DEA intruded beyond Federal Express's initial invasion, then the Fourth Amendment was triggered "with respect to which the expectation of privacy has not already been frustrated."[292]

Jacobsen then specified two distinct intrusions the DEA committed: 1) the DEA agents "removed the tube from the box, the plastic bags from the tube and a trace of powder from the innermost bag," and 2) they "made a chemical test of the powder."[293] The DEA's first intrusion involving opening the package and picking up the tube gave the government no information it had not learned from the Federal Express employees.[294] The

286. *Id*.

287. *Id*. at 111–12.

288. *Id*. at 115.

289. *Id*.

290. *Id*. at 117.

291. *Id*.

292. *Id*. *Jacobsen* noted, "In such a case the authorities have not relied on what is in effect a private search, and therefore presumptively violate the Fourth Amendment if they act without a warrant." *Id*. at 117–18.

293. *Id*. at 118.

294. *Id*. at 118–119.

defendants "could have no privacy interest in the contents of the package, since it remained unsealed and since the Federal Express employees had just examined the package and had, of their own accord, invited the federal agent to their offices for the express purpose of viewing its contents."[295] Likewise, the DEA's removal of the bags from the tube and visually inspecting them "enabled the agent to learn nothing that had not previously been learned during the private search."[296]

The Court also analyzed the DEA's second intrusion "occasioned by the field test, which had not been conducted by the Federal Express agents and therefore exceeded the scope of the private search."[297] Since a Fourth Amendment search required government intrusion on a privacy expectation that was "reasonable"—or "legitimate"—*Jacobsen* viewed the field test intrusion through the prism of what interests could be considered "legitimate."[298] Society need not recognize as "legitimate" information regarding "wrongful" behavior, such as burglar's presence in an empty cabin.[299] The DEA's "chemical test," which merely disclosed the existence of cocaine—a substance illegal to possess—did not implicate "any legitimate interest in privacy."[300]

Thus, *Walter* and *Jacobsen's* key point was that the amount of Fourth Amendment protection from a government intrusion depended on the scope of any earlier private invasion. *Walter* only found fault when the FBI went beyond the prior private search—opening the package and viewing the explicit drawings and pictures on the boxes within them—by actually watching the films.[301] In short, the test was framed by the extent of the "the antecedent private search."[302] This analysis could open a path to admission for evidence from genetic genealogical sites. When a person, on his or her own initiative, provides a saliva sample to a commercial site, such as 23andMe, and then uploads the results to an open genealogical site, such as GEDmatch, the individual is essentially exposing the portions of his or her DNA shared with relatives. Much as *Walter's* L'Eggs employees opened the package or *Jacobsen's* Federal Express employees cut the tube, the individual family member uploading his genetic information tears open

295. *Id.* at 119.
296. *Id.* at 119–120.
297. *Id*. at 122.
298. *Id*.
299. *Id*.
300. *Id*. at 123.
301. *Walter*, 447 U.S. at 651–52, 658.
302. *Jacobsen*, 466 U.S. at 116.

segments of the DNA of all of his or her relatives to public view. When investigators later obtain this genetic information from GEDmatch, this initial collection itself goes no further than the original "antecedent private search."[303]

The only question remaining is whether government use of the DNA information in forming family trees and in comparing genes with crime scene samples amounts to a further official intrusion akin to the FBI watching the film from the opened box in *Walter*.[304] The investigation techniques used to locate the Golden State Killer suspect after visiting GEDmatch do not seem likely to be considered further intrusions on par with viewing the film in *Walter*. Hole's subsequent investigation in pursuit of DeAngelo involved only old-fashioned gumshoe detective work into public information. Reviews of census records, gravesite locators, and old newspaper obituaries involve only the examination of information available to anyone wishing to view it.[305] The "antecedent private search" precedent could thus provide law enforcement with a door through which it might get genetic genealogy evidence admitted despite the lack of a warrant.

Any person challenging evidence from a relative that the government has obtained from a genealogical site will have to establish "standing," or the personal right to challenge the particular Fourth Amendment violation.

Suppose the government acknowledged that its search for the Golden State Killer suspect's distant relative on a genealogical site violated the Fourth Amendment. Would such concession help the suspect exclude the results of this genealogical search from court? It could be argued that the person who could claim invasion of privacy from the genealogical visit is not the suspect but the relative who's DNA was the subject of state scrutiny. Any link to the suspect came only from DNA the suspect left—or essentially abandoned—at the crime scene as semen, blood, or other biological material. As previously noted, the later tracing from a distant relative's common ancestor—the great, great, great, grandparent—involved[306] traditional types of investigation, such as looking at gravesites

303. *Id*.

304. The DEA's field test of the powder in *Jacobsen*, unlike the FBI search in *Walter*, was found to not implicate a "legitimate" expectation of privacy. *Id*. at 123.

305. Jouvenal, TO FIND ALLEGED GOLDEN STATE KILLER, supra note 2, at 2. Officials also examined "police and commercial databases." *Id*. While law enforcement's reference to its own databases should not trigger a Fourth Amendment issue, the privacy concerns surrounding use of "commercial" databases would depend on the specifics involved in each particular visit. *Id.*

306. Winton, *supra* note 60.

and checking newspapers and census records,[307] which would raise no Fourth Amendment red flags. This issue, commonly referred to as "standing,"[308] involves the question of who precisely has the right to contest a particular Fourth Amendment violation.[309]

One of the most significant cases on the issue of "standing," or the right to contest a Fourth Amendment search, is *Rakas v. Illinois*, a case which altered even the language employed in this area of the law.[310] In *Rakas*, officers, suspecting a stopped car of being involved in a robbery, ordered its occupants out of the vehicle.[311] When Rakas and two others then exited the vehicle, the officers searched the car, discovering "a box of rifle shells in the glove compartment, which had been locked, and a sawed-off rifle under the front passenger seat."[312] Rakas moved to suppress these items as recovered during an unlawful search.[313] The trial court ruled Rakas lacked standing to contest the search because he, being merely a passenger, did not own the car and further did not claim ownership of the gun or shells.[314]

Rakas described the "concept of standing" as focusing on "whether the person seeking to challenge the legality of a search as a basis for suppressing evidence was himself the 'victim' of the search or seizure."[315] "Standing" involved two questions: "first, whether the proponent of a particular legal right has alleged "injury in fact," and, second, whether the proponent is asserting his own legal rights and interests rather than basing his claim for relief upon the rights of third parties."[316] *Rakas*, however, was less than pleased with the "'standing' terminology"[317] because such language caused the issue to be falsely seen as "theoretically distinct from the merits of a defendant's Fourth Amendment claim."[318] The Court concluded that the "definition" of Fourth Amendment rights was "more

307. Jouvenal, *supra* note 2, at 2.

308. The Court, in *Byrd v. United States*, commented, "It is worth noting that most courts analyzing the question presented in this case . . . have described it as one of Fourth Amendment 'standing.'" 138 S. Ct. 1518, 1530 (2018).

309. Rakas v. Illinois, 439 U.S. 128, 133 (1978).

310. *Id.*

311. *Id.* at 130.

312. *Id.*

313. *Id.* at 130.

314. *Id.*

315. *Id.* at 132.

316. *Id.* at 139.

317. *Id.* at 133.

318. *Id.*

properly placed within the purview of substantive Fourth Amendment law than within that of standing."[319]

Rakas deemed Fourth Amendment rights as "personal rights" that could "not be vicariously asserted."[320] The Court ruled, "A person who is aggrieved by an illegal search and seizure only through the introduction of damaging evidence secured by a search of a third person's premises or property has not had any of his Fourth Amendment rights infringed.[321] Only those "whose Fourth Amendment rights have been violated" could seek exclusion of the evidence obtained from that violation.[322] Rakas contested the search of the glove compartment and the space under the car's seat, yet he did not claim that he had "any legitimate expectation of privacy" in these areas.[323] Lacking a reasonable privacy expectation, Rakas necessarily lacked a Fourth Amendment right in the car, and therefore could not contest the police illegality. In terms that Rakas would have disapproved, he lacked "standing" to claim the officer's search of the car violated his Fourth Amendment rights.

In the next case involving the right to contest a search of a vehicle, *Byrd v. United States*, the Court had mellowed its stance on the terminology of "standing" by noting, "The concept of standing in Fourth Amendment cases can be a useful shorthand for capturing the idea that a person must have a cognizable Fourth Amendment interest in the place searched before seeking relief for an unconstitutional search."[324] In *Byrd*, Terrence Byrd and Latasha Reed drove in Byrd's Honda to Budget car rental in New Jersey. Reed then entered the agency and rented a car while Byrd stayed outside in his Honda. After signing a rental contract that explicitly provided, "PERMITTING AN UNAUTHORIZED DRIVER TO OPERATE THE VEHICLE IS A VIOLATION OF THE RENTAL AGREEMENT," Reed handed the rental's keys to Byrd, who drove off in the rental car.[325] Later, a Pennsylvania trooper stopped Byrd as he was driving the rental car to Pittsburgh.[326] The officer noticed when he approached the car, Byrd was so nervous that he "was shaking and had a

319. *Id.* at 140.
320. *Id.* at 133–34.
321. *Id.* at 134.
322. *Id*.
323. *Id.* at 150, n. 17.
324. *Byrd*, 138 S. Ct. at 1530.
325. *Id.* at 1524.
326. *Id*.

hard time obtaining his driver's license."[327] Another officer then arrived at the scene.[328] When the troopers learned Byrd was not listed as an authorized driver on the rental agreement, they told him they could search the car without consent. The resulting search of the car's trunk revealed "body armor and 49 bricks of heroin," exposing Byrd to federal drug charges.[329]

When presented with this case, the *Byrd* Court asked, "Does a driver of a rental car have a reasonable expectation of privacy in the car when he or she is not listed as an authorized driver on the rental agreement?"[330] While noting that the legitimacy of privacy expectations "must have a source outside of the Fourth Amendment," *Byrd* identified two such sources: 1) "concepts of real or personal property law," and 2) "understandings that are recognized and permitted by society."[331] Relying on the "general property-based concept," the Court determined that Byrd was the "sole occupant" of the car and therefore "could exclude others from it."[332] *Byrd* declared, "one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of [the] right to exclude."[333] Acknowledging that Byrd "violated the rental agreement," the Court dismissed this fact because, "As anyone who has rented a car knows, car-rental agreements are filled with long lists of restrictions."[334] "Few would contend," urged the Court, that violating such provisions as driving on an unpaved road or while holding a cellphone, "has anything to do with a driver's reasonable expectation of privacy in the rental car."[335] *Byrd* therefore held, "the mere fact that a driver in lawful possession or control of a rental car is not listed on the rental agreement will not defeat his or her otherwise reasonable expectation of privacy."[336]

327. *Id*.

328. *Id*.

329. *Id.* at 1523.

330. *Id.* at 1527. Deciding whether Byrd had "his own Fourth Amendment rights infringed by the search" meant determining whether he had a "legitimate expectation of privacy" in the place searched. *Id.* at 1526.

331. *Id.* at 1527. The "understandings that are recognized and permitted by society" will not be explored in this Article in light of the previous discussions regarding privacy expectations in *supra* Section B of Part IV and "widely shared social expectations" in *supra* Section C of Part IV.

332. *Id.* at 1527, 1528.

333. *Id.* at 1528.

334. *Id.* at 1529.

335. *Id*.

336. *Id.* at 1531.

Byrd, in applying property law principles to determine whether a person possessed the reasonable expectation of privacy to contest a search, offered another test that could be used to consider the admissibility of evidence obtained from genealogy sites. Through *Byrd's* lens, asking whether a person has standing to challenge a government visit of a family member's genealogy site amounts to inquiring whether that person has a property right enabling him or her to exclude others from the site. The design and operation of GEDmatch undermines any such ability to exclude. In its "Terms of Service and Privacy Policy," GEDmatch alerts potential users, "GEDmatch exists to provide DNA and genealogy tools for comparison and research purposes."[337] The comparison and research that GEDmatch mentions are collaborative processes that can only work by sharing information. The sites' very existence, along with the million uploads made on it, demonstrate the inability to exclude others.[338] GEDmatch further notes, "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."[339] The site's terms of service, in twice explicitly referencing sharing, again show a lack of property interest by a relative in excluding others. Finally, GEDmatch explains, "Raw DNA data uploaded to GEDmatch.Com ('Raw Data') remains the property of the person who uploaded it."[340] In this statement, the only property interest GEDmatch acknowledges is that of the person uploading the DNA, not the relatives who might contest the viewing of it. Under *Byrd's* "general property-based concept," without a right to exclude, one has no property interest, without a property interest, one has no reasonable expectation of privacy, and without such a privacy expectation, one has no standing.[341] Since a relative cannot exclude others from GEDmatch's site, his or her standing fails at the outset.

337. *GEDmatch.Com Terms of Service and Privacy Policy*, GEDMATCH, https://www.gedmatch.c om/tos.htm (last modified May 20, 2018).

338. Jouvenal et al., *supra* note 62.

339. *GEDmatch.Com Terms of Service and Privacy Policy*, GEDMATCH, https://www.gedmatch.com/tos.htm (last modified May 20, 2018).

340. *Id*.

341. *Byrd*, 138 S. Ct. at 1528.

Conclusion

Facing the daunting realization that there are "200,000-plus cold cases in the United States," Kenneth Mains, "founder of the American Investigative Society of Cold Cases," has argued that any resource which helps close such cases "needs to be utilized."[342] The National District Attorneys Association's Josh Marquis wondered, "Why in God's name would we come up with a reason that we are not able to use" these genetic websites?[343] While law enforcement is keenly aware of the potential "investigative goldmine" of these databases, the persons who use them "aren't really thinking through the implications of creating this treasure trove of data that can be mined."[344] University of Michigan law professor Barbara McQuade has noted that for most people, DNA is so "very private, very personal" that "even if you have given it up to one of these third-party services, maybe there should be a higher level of security."[345] There thus exists a gap between the perceptions of investigators zealously pursuing criminals and laypersons who have not considered the full consequences of this rapidly advancing technology. It is in this gap that Fourth Amendment rights, not fully appreciated by those using genealogical websites, might fall.

Further, full privacy protection from government use of genetic genealogy might be beyond the volitional power of any one individual. Those who, after educating themselves on every aspect of genealogical privacy, choose to forgo uploading their own DNA, might still find their genetic information probed by the government. "Even if we've never spit into a test tube, some of our genetic information may be public—and accessible to law enforcement."[346] There is no getting around the fact that any person, upon submitting DNA information to a public genealogy site, exposes the DNA of his or her relatives, even if "distant" or "far flung."[347] This breach occurs regardless of the consent or even the knowledge of thousands.

If confronted with the Fourth Amendment issues of genetic genealogy, the Court could address the concerns created by this new technology in a variety of ways. The Court could turn to its earlier case

342. Jouvenal et al., *supra* note 62.

343. *Id*.

344. *Id*.

345. *Id.*

346. Gafni, *supra* note 57.

347. *Id*.

involving DNA collection of arrestees entering custody, *Maryland v. King*. Such an approach would bear so little fruit, due to the narrowness of *King's* ruling, that the Court would have to craft a new rule for the entirely separate issue of government collection of DNA information on the Internet.[348] The Court could analyze genetic genealogy's privacy issues by considering *Carpenter's* latest application of the third-party doctrine.[349] The force of *Carpenter's* reasoning would likely cause the Court to view genetic genealogy as so sophisticated and the information it handled as so sensitive that a government visit to a genealogy site would be deemed a Fourth Amendment search requiring a warrant.[350] The Court could consider a person's uploading of DNA information as amounting to a grant of consent to search the portions of his or her genome held in common with relatives. Then, the third-party consent precedent's "widely shared social expectations" would likely reject government use of DNA information without a warrant.[351] Two other Fourth Amendment doctrines, *Walter* and *Jacobsen's* "antecedent private search" rule[352] and *Byrd's* "general property-based concept" definition of standing, offer law enforcement with potential avenues for admission of genetic genealogy evidence.[353] Should the Court deem a person's upload of DNA information onto a genealogy site to be a prior private search, then *Walter* and *Jacobsen* would permit the government to explore this same genetic information—previously exposed by a private person—without a warrant. Finally, following *Byrd's* reasoning, the government could avoid the exclusion of evidence obtained in visiting a genealogy site even if the warrantless download of genetic information was found to violate the Fourth Amendment. Since the family member could not exclude others from visiting the genealogy site, he or she could not establish a property interest sufficient to support standing to challenge the search in the first place.[354] The Court's decision about the Fourth Amendment reasonableness of warrantless government collection of genetic information from genealogy sites will thus turn on how it chooses to frame the question triggered by this new technology. When it comes to genetic genealogy, as with much else in the world of heredity, where you end up all depends on where you start.

348. *King*, 569 U.S. at 449, 462.
349. *Carpenter*, 138 S. Ct. at 2223.
350. *Id*.
351. *Randolph*, 547 U.S. at 111.
352. *Jacobsen*, 466 U.S. at 116.
353. *Byrd*, 138 S. Ct. at 1528.
354. *Id*.

***