Loyola of Los Angeles Law Review

Volume 53 | Number 4 Article 5

Summer 8-1-2020

A Too Permeating Police Surveillance: Consumer Genetic Genealogy and the Fourth Amendment After Carpenter

Michael I. Selvin

A TOO PERMEATING POLICE SURVEILLANCE: CONSUMER GENETIC GENEALOGY AND THE FOURTH AMENDMENT AFTER *CARPENTER*

*Michael I. Selvin**

I. INTRODUCTION

On April 24, 2018, in Sacramento, California police arrested Joseph James DeAngelo, seventy-two, a grandfather and retired police officer, believing him to be the long sought-after Golden State Killer.[1] DeAngelo is suspected of having committed twelve homicides and more than fifty rapes, and has been linked to more than 175 crimes.[2] Prosecutors in Sacramento have charged him with twenty-six counts of murder and kidnapping.[3]

The Golden State Killer, also known as the East Area Rapist, terrorized the Sacramento County area during his ten-year spree, from 1976 to 1986.[4] He wore a mask and bound his victims, beginning first with single women and moving on to married couples, often raping women in front of their husbands before killing them both.[5] He

* J.D. Candidate, May 2020, Loyola Law School, Los Angeles; B.A., Government, Dartmouth College, June 2007. Special thanks to Professor Kevin Lapp for his invaluable guidance and feedback throughout the writing process.

1. T.J. Ortenzi, *Hunt for Golden State Killer Led Detectives to Hobby Lobby for DNA Sample*, WASH. POST (June 1, 2018, 10:53 PM), https://www.washingtonpost.com/news/post-nation/wp/2018/06/02/hunt-for-golden-state-killer-led-detectives-to-hobby-lobby-for-dna-sample/?utm_term=.f091adc76.

2. *Id.*; *Golden State Killer Suspect Joseph DeAngelo Arrested in Sacramento*, ABC7 EYEWITNESS NEWS (Apr. 26, 2018), https://abc7chicago.com/golden-state-killer-joseph-james-deangelo-east-area-rapist-arrested/3390783/.

3. Associated Press, *DNA Clears Accused Golden State Killer Joseph DeAngelo of 1975 Murder*, NBC NEWS (Jan. 9, 2019, 5:37 AM), https://www.nbcnews.com/news/us-news/dna-clears-accused-golden-state-killer-joseph-deangelo-1975-murder-n956566. Prosecutors charged the kidnapping counts because the statute of limitations had run on the rape cases. *Id.*

4. *Golden State Killer Suspect Joseph DeAngelo Charged with 13 Murders*, SKY NEWS (Aug. 24, 2018), https://news.sky.com/story/golden-state-killer-suspect-joseph-deangelo-charged-with-13-murders-11480597.

5. Thomas Fuller, *How a Genealogy Site Led to the Front Door of the Golden State Killer*, N.Y. TIMES (Apr. 26, 2018), https://www.nytimes.com/2018/04/26/us/golden-state-killer.html.

abruptly ended his spree, investigators believe, in 1986.[6] It is unclear why.[7]

Police had recovered DNA evidence belonging to the perpetrator of numerous crimes now linked to DeAngelo, but at the time could not match the samples to any suspects.[8] The case went cold for four decades, but investigators had not given up.[9] Sacramento cold case detective Paul Holes hired Barbara Rae-Venter, a retired patent attorney from California who made a hobby of helping adopted people find their birth parents using commercial genealogy websites.[10] Investigators created a profile of the unknown perpetrator's DNA and uploaded the profile to GEDmatch, an online commercial genealogy database intended to allow users to upload their own genetic profiles and search for unknown relatives.[11] Rae-Venter ran a search of the suspected perpetrator's DNA profile against the nearly one million user profiles then comprising GEDmatch's database,[12] and identified several users who were third cousins of the source of the cold case DNA.[13]

Holes and Rae-Venter then started building family trees around these third cousins, attempting to find a common ancestor.[14] In all, it took a team of five investigators four months to identify DeAngelo.[15] Finding a common ancestor proved difficult, as many of the suspect's

---

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

7. *Id.*

8. *Id.*

9. *Id.*

10. Heather Murphy, *She Helped Crack the Golden State Killer Case. Here's What She's Going to Do Next*, N.Y. TIMES (Aug. 29, 2018), https://www.nytimes.com/2018/08/29/science/barbara-rae-venter-gsk.html.

11. *See id.*

12. As of November 2019, the GEDmatch database had 1.3 million user profiles. Kashmir Hill & Heather Murphy, *Your DNA Profile Is Private? A Florida Judge Just Said Otherwise*, N.Y. TIMES (Nov. 5, 2019), https://www.nytimes.com/2019/11/05/business/dna-database-search-warrant.html?smid=nytcore-ios-share (last updated Dec. 30, 2019).

13. Jocelyn Kaiser, *We Will Find You: DNA Search Used to Nab Golden State Killer Can Home in on About 60% of White Americans*, SCI. MAG. (Oct. 11, 2018, 2:00 PM), https://www.sciencemag.org/news/2018/10/we-will-find-you-dna-search-used-nab-golden-state-killer-can-home-about-60-white.

14. Murphy, *She Helped Crack the Golden State Killer Case*, *supra* note 10.

15. Jouvenal, *supra* note 6.

relatives were recent Italian immigrants, preventing the team from tracing their lineages farther back.[16] The team had more success investigating relatives on the English side of the identified individuals' lineages and eventually was able to formulate rough family trees.[17]

Utilizing birth and death certificates, marriage records, social media profiles, census data, and news stories, Rae-Venter and her team eventually traced twenty-five family trees back to a common ancestor, a great-great-great grandparent of both the GEDmatch users identified in the search and the source of the forensic DNA.[18] They then worked forward from the common ancestor, looking for relatives in the lineage who fit the profile of the Golden State Killer based on his approximate age when the crimes were committed and his residency in or near Sacramento.[19]

Numerous suspects emerged, including DeAngelo.[20] Rae-Venter used a DNA analytics tool on GEDmatch that predicted the killer's DNA likely belonged to someone with blue eyes.[21] She also used a health risk analysis website called Promethease.com to determine that the suspect likely began balding prematurely.[22] Of the suspects Rae-Venter's team had honed in on, only DeAngelo had blue eyes and a receding hairline.[23]

Sacramento detectives then surveilled DeAngelo's home for three days.[24] On April 18, 2018, they followed him to a Hobby Lobby store in Roseville, California.[25] While he was in the store, investigators swabbed the handle of his car for DNA and sent it to the crime lab.[26] They also removed a tissue from his garbage and sent it to a crime lab for DNA testing.[27] Both samples matched DNA collected from the scene of a rape and murder in 1980 that was long suspected of having been committed by the Golden State Killer.[28] Police arrested

16. Murphy, *She Helped Crack the Golden State Killer Case*, *supra* note 10.
17. *Id.*
18. *Id.*; Jouvenal, *supra* note 6.
19. Jouvenal, *supra* note 6.
20. *Id.*
21. Murphy, *She Helped Crack the Golden State Killer Case*, *supra* note 10.
22. *Id.*
23. *Id.*
24. Ortenzi, *supra* note 1.
25. *Id.*
26. *Id.*
27. *Id.*
28. *Id.*

DeAngelo days later, and a DNA sample taken upon arrest matched more than ten cold case murders in California.[29]

Whether genetic genealogical investigations utilizing commercial databases by law enforcement implicate the Fourth Amendment's prohibition on unreasonable searches and seizures is an open question. Indeed, it is difficult to neatly apply traditional Fourth Amendment doctrine to the technique to even determine whether such investigations would qualify as searches subject to the Fourth Amendment. Under the traditional third-party doctrine, databased individuals would not have a reasonable expectation of privacy in their genetic data voluntarily uploaded to publicly available databases.[30] But what about the relatives of these individuals, both the intermediate relatives on a given family tree between the database user and the source of the forensic DNA sample, and the suspect ultimately identified by the investigation? Genetic information is shared amongst relatives, and in a given investigation, genetic and other highly intimate personal information is revealed. Does the technique constitute a search of database users' relatives who did not voluntarily provide their genetic information to any database? And as the use of this method of investigation continues to grow, with no guidelines and little oversight,[31] what safeguards and limits should be imposed?

This Note begins with an explanation of how genetic genealogical investigations are conducted and discusses the technique's rapid development and use in criminal investigations nationwide after DeAngelo's arrest was announced. Part III provides an overview of traditional uses of DNA in criminal investigations utilizing the FBI's Combined DNA Index System (CODIS): direct-match searching and the more controversial, and less widely accepted, partial-match familial searching. Part III further explains why the constitutional underpinnings of CODIS do not apply to commercial genetic genealogical investigations. Part IV considers whether genetic genealogical investigations would be considered constitutional searches under traditional Fourth Amendment doctrine and under the

29. Fuller, *supra* note 5.

30. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

31. Sarah Zhang, *The Messy Consequences of the Golden State Killer Case*, ATLANTIC (Oct. 1, 2019), https://www.theatlantic.com/science/archive/2019/10/genetic-genealogy-dna-database-criminal-investigations/599005/.

Supreme Court's recent decision in *Carpenter v. United States*.[32] Assuming that genetic genealogical investigations are constitutional searches, Part IV then discusses whether such searches are lawful and under what circumstances. Last, Part V argues that effective legislation must be enacted to place limits on law enforcement use of the technique and highlights a number of factors and policy considerations that must be carefully weighed and considered in crafting any such legislation.

II. BACKGROUND

A. GEDmatch

Amongst commercial genealogy websites, GEDmatch has emerged as law enforcement's favorite for criminal investigations.[33] It functions differently than its higher profile counterparts, such as Ancestry and 23andMe.[34] Ancestry and 23andMe prohibit use of their services by law enforcement entirely,[35] whereas GEDmatch currently allows law enforcement to search profiles of consenting users for certain crimes and until recently granted law enforcement access to all user profiles to investigate violent crimes.[36] And the process by which an Ancestry or 23andMe user creates his or her DNA profile makes these sites more difficult for law enforcement to utilize than GEDmatch.[37] Most DNA testing services require users to mail in a sample of their saliva in a standardized container, which the service then analyzes in its own lab to create a DNA profile that is uploaded to the site.[38] It would be difficult for law enforcement to utilize such

32. 138 S. Ct. 2206 (2018).

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

34. Fuller, *supra* note 5.

35. Kate Snow & Jon Schuppe, *'This is Just the Beginning': Using DNA and Genealogy to Crack Years-Old Cold Cases*, NBC NEWS (July 18, 2018, 1:30 AM), https://www.nbcnews.com/news/us-news/just-beginning-using-dna-genealogy-crack-years-old-cold-cases-n892126.

36. Zhang, *supra* note 31.

37. Murphy, *How an Unlikely Family History Website Transformed Cold Case Investigations*, *supra* note 33.

38. Fuller, *supra* note 5.

services because they will not accept blood or semen samples,[39] crime scene evidence, or DNA profiles generated in other labs.[40]

GEDmatch, based out of a small house in Florida owned by one of its founders, functions very differently.[41] It has no lab.[42] Instead, it allows users to upload DNA profiles generated elsewhere, without regard for the DNA's source or the reliability of the labs in which DNA profiles were originally tested.[43] GEDmatch is different from its competitors in that it is not a DNA testing service, but a publicly searchable database that allows users who have had their DNA analyzed elsewhere to more deeply investigate their ancestry.[44]

GEDmatch is also better equipped than other services for criminal investigations due to the technology employed by the site itself. GEDmatch analyzes autosomal DNA single nucleotide polymorphisms, which are passed down by both males and females along all ancestral lines.[45] This type of DNA data allows for comparison of any two individuals regardless of how they are related.[46] GEDmatch searches hundreds of thousands of DNA markers, looking for long stretches that match, thus indicating familial ties.[47] GEDmatch allows users to see precisely where these segments of their DNA overlap with those of their relatives and to what extent.[48] In this way, a user can determine not only to whom on the site they are related, but *how*.[49] GEDmatch can consistently match relatives as distant as third cousins and, to a professionally trained genealogist, convey crucial information regarding how they are related.[50] A recent

39. *See id.*

40. *See* Murphy, *How an Unlikely Family History Website Transformed Cold Case Investigations*, *supra* note 33.

41. *Id.*

42. *See id.*

43. Fuller, *supra* note 5.

44. Murphy, *How an Unlikely Family History Website Transformed Cold Case Investigations*, *supra* note 33.

45. *How Genetic Genealogy Works*, PARABON NANOLABS, https://snapshot.parabon-nanolabs.com/intro#genealogy-how (last visited Apr. 5, 2020); *see Concepts—CentiMorgans SNPs and Pickin' Crab*, DNAEXPLAINED, https://dna-explained.com/2016/03/30/concepts-centimorgans-snps-and-pickin-crab/ (last visited Apr. 5, 2020).

46. *How Genetic Genealogy Works*, *supra* note 45.

47. *Id.*

48. Murphy, *How an Unlikely Family History Website Transformed Cold Case Investigations*, *supra* note 33.

49. *Id.*

50. *Id.*

study determined that the technology could narrow down the identity of an anonymous source of DNA to less than twenty potential individuals in a database of 1.3 million utilizing nothing but the sample and an approximate age.[51]

B. Genealogy Experts

While GEDmatch's analytics are highly effective, the data it provides are relatively useless for solving cold cases without the assistance of a trained genealogy expert.[52] One such expert, CeCe Moore of Parabon Nanolabs, has recently emerged among the experts most commonly used by law enforcement and, following numerous television and press interviews, has become a public face of genetic genealogy criminal investigations.[53]

Parabon Nanolabs is based out of Reston, Virginia, and is comprised of roughly twenty employees.[54] In 2011, in conjunction with the Department of Defense, Parabon developed its first program to assist law enforcement in cold case investigations.[55] Parabon's lab would analyze cold case DNA samples to create computer-generated sketches of what their owners might look like.[56] Hundreds of police departments signed up for the service.[57] As the program continued to grow, Parabon developed technology to analyze and compare autosomal DNA from samples submitted to its lab in an effort to identify people based on distant relatives.[58] Following the publicity surrounding Joseph DeAngelo's arrest as the Golden State Killer, Parabon hired Moore, a traditional genealogist, and began offering its services to police departments to employ the same genetic genealogy investigative techniques used to identify DeAngelo to solve other cold cases.[59]

---

51. Kaiser, *supra* note 13.

52. Murphy, *How an Unlikely Family History Website Transformed Cold Case Investigations*, *supra* note 33.

53. Snow & Schuppe, *supra* note 35.

54. *Id.*

55. *Id.*

56. *Id.*

57. *Id.*

58. *Id.*

59. Megan Molteni, *The Future of Crime-Fighting Is Family Tree Forensics*, WIRED (Dec. 26, 2018, 8:00 AM), https://www.wired.com/story/the-future-of-crime-fighting-is-family-tree-forensics/.

Police departments send cold case DNA samples to Parabon, which processes the samples in its lab and creates autosomal DNA profiles in a format compatible with GEDmatch.[60] Parabon uploads these profiles to GEDmatch, and Moore searches the database for relatives.[61] As in the Golden State Killer investigation, Moore builds family trees of each identified relative backward in time until she finds a common ancestor, using public records such as marriage and birth certificates, obituaries, social media profiles, census records and news articles.[62] She then works forward until she arrives at potential suspects in the family lineage that fit the perpetrator's profile.[63] These suspects are then given to the police to investigate further.[64]

While the initial investigation of DeAngelo took thousands of law enforcement man-hours, the process has been refined and streamlined, and is rapidly becoming much more efficient.[65] Parabon has said it finds partial matches to cold case DNA samples on GEDmatch in 60 percent of its cases and expects that rate to grow as more people upload their genetic profiles to the site.[66]

C. Aftermath of the Golden State Killer Case

In just over a year, use of this technique by law enforcement has grown at exponential rates.[67] Parabon has helped solve numerous cold cases in recent months, including the 1988 murder of an eight-year-old girl in Indiana, the 1987 killing of a couple in Washington, and the 1992 homicide of a woman in Pennsylvania.[68] Genealogists have identified over forty cold case suspects since Joseph DeAngelo.[69]

The technique has become much more efficient as well, producing results at ever-increasing speed. In September, 2018, Sacramento police identified Roy Charles Waller as the suspect in the commission of ten unsolved rapes by uploading his DNA profile to

60. *Id.*
61. *Id.*
62. *Id.*
63. Snow & Schuppe, *supra* note 35.
64. *Id.*
65. Murphy, *How an Unlikely Family History Website Transformed Cold Case Investigations*, *supra* note 33; Murphy, *She Helped Crack the Golden State Killer Case*, *supra* note 10.
66. Snow & Schuppe, *supra* note 35.
67. *Id.*
68. *Id.*
69. Zhang, *supra* note 31.

GEDmatch and identifying a close relative.[70] His arrest was only the fifteenth instance GEDmatch was used to solve a cold case following DeAngelo's arrest,[71] and investigators identified Waller as their suspect within mere hours of uploading his DNA to GEDmatch.[72]

Yet the widespread use of the technique by law enforcement, with little formal oversight, has sparked user backlash and bitter debate within the genealogical community.[73] User backlash caused by GEDmatch's decision to break its own terms of service led it to overhaul its policy regarding law enforcement use of the database entirely.[74] Prior to May 18, 2019, GEDmatch's terms of service disclosed to its users that it accepted "DNA obtained and authorized by law enforcement to either: (1) identify a perpetrator of a violent crime against another individual; or (2) identify remains of a deceased individual."[75] GEDmatch defined "violent crime" as "homicide or sexual assault."[76] However, in November 2018, GEDmatch allowed law enforcement access to investigate a lesser crime.[77] Detectives in Centerville, Utah were investigating the attack of a seventy-one-year-old woman, who was choked by her assailant until she lost consciousness but survived.[78] She was not sexually assaulted.[79] When Parabon informed the detectives they could not upload the DNA found at the scene to GEDmatch because the attack did not constitute a violent crime under GEDmatch's terms of service, the detectives approached Curtis Rogers of GEDmatch and Steven Armentrout of

70. Murphy, *How an Unlikely Family History Website Transformed Cold Case Investigations*, *supra* note 33.

71. *Id.*

72. *Id.*

73. Zhang, *supra* note 31.

74. Peter Aldhous, *This Genealogy Database Helped Solve Dozens of Crimes. But Its New Privacy Rules Will Restrict Access by Cops*, BUZZFEED NEWS (May 19, 2019, 4:51 PM), https://www.buzzfeednews.com/article/peteraldhous/this-genealogy-database-helped-solve-dozens-of-crimes-but.

75. *GEDMatch.Com Terms of Service and Privacy Policy*, GEDMATCH, https://web.archive.org/web/20190506040926/https://www.gedmatch.com/tos.htm (last visited May 6, 2019) (version prior to May 18, 2019 update).

76. *Id.*

77. Pat Reavy, *Plastic Milk Container, Genealogy Helped Utah Police Crack Church Assault Case*, KSL.COM (May 13, 2019, 3:42 PM), https://www.ksl.com/article/46551323/plastic-milk-container-genealogy-helped-utah-police-crack-church-assault-case.

78. *Id.*

79. *See id.*

Parabon for permission.[80] They consented, and Parabon's genealogists were able to trace the DNA sample to a great-uncle of the source and ultimately to the source himself.[81] In April 2019, he was arrested and charged with aggravated assault and aggravated burglary.[82]

Mere days after news broke of the Utah investigation, user backlash caused GEDmatch to revise its terms of service.[83] It now allows law enforcement to upload DNA "to identify a perpetrator of a violent crime against another individual, where 'violent crime' is defined as murder, nonnegligent manslaughter, aggravated rape, robbery, or aggravated assault."[84] However, GEDmatch created new privacy settings for its DNA profiles. Users' profiles are all set to private by default, restricting their data from ever being found in a search. They can then choose to change their privacy preference to "Public + opt-out," in which "DNA data is [sic] available for comparison to any Raw Data in the GEDmatch database, except DNA kits identified as being uploaded for law enforcement purposes," or to "Public + opt-in," allowing for matches to DNA uploaded by law enforcement.[85]

Because all GEDmatch users now have to affirmatively opt-in, many profiles are beyond law enforcement's reach, greatly diminishing the efficacy of the technique, at least for now. Thus far, only 185,000 of GEDmatch's 1.3 million users have chosen to opt-in,[86] greatly hindering its utility in criminal investigations.[87] While this approach may temporarily allay concerns about law enforcement intrusion into millions of people's private genetic information, it returns some level of control over such information to GEDmatch's users only. It does nothing to address the legitimate privacy interests of the relatives of users who choose to opt-in—millions of people who

80. Peter Aldhous, *The Arrest of a Teen on an Assault Charge Has Sparked New Privacy Fears About DNA Sleuthing*, BUZZFEED NEWS (May 14, 2019, 10:15 PM), https://www.buzzfeednews.com/article/peteraldhous/genetic-genealogy-parabon-gedmatch-assault.

81. *Id.*

82. *Id.*

83. *Id.*

84. *GEDMatch.Com Terms of Service and Privacy Policy*, GEDMATCH, https://www.gedmatch.com/tos.htm (last updated Dec. 9, 2019).

85. *Id.*

86. Hill & Murphy, *supra* note 12.

87. Zhang, *supra* note 31.

have never uploaded their DNA to the site, nor consented to have their genetic information implicated in criminal investigations. Users, therefore, decide whether or not law enforcement can access not only their own genetic information, but that of their extended family as well.

Whether such investigations intrude on the protected Fourth Amendment interests of these relatives, including relative-suspects ultimately identified through this technique, is currently an open question. William Talbott II was convicted in June 2019 of the 1987 murder of a young Canadian couple.[88] Investigators identified Mr. Talbott by utilizing GEDmatch and Parabon, yet his defense attorneys never challenged the constitutionality of the technique at trial.[89] Rachel Forde, Mr. Talbott's Snohomish County public defender, stated she felt the evidence was not relevant because police only used it to generate a lead, not to support probable cause to obtain the arrest warrant, and it was not introduced at trial.[90] Indeed, the technique does not fit neatly into the traditional Fourth Amendment analytical framework, nor does the Supreme Court's reasoning for finding CODIS searches constitutional apply.

III. FORENSIC DNA IN CRIMINAL INVESTIGATIONS

The use of DNA by law enforcement in criminal investigations is common nationwide. Two techniques utilizing forensic DNA databases were well established prior to the advent of commercial genealogy investigations: direct-match searching and partial-match familial searching. Both utilize CODIS, a software program authorized by Congress and supervised by the FBI, which allows law enforcement to search numerous state and national databases of arrestee DNA profiles.[91]

88. Heather Murphy, *Genealogy Sites Have Helped Identify Suspects. Now They've Helped Convict One*, N.Y. TIMES (July 1, 2019), https://www.nytimes.com/2019/07/01/us/dna-genetic-genealogy-trial.html.

89. *Id.*

90. Jason Tashea, *Genealogy Sites Give Law Enforcement a New DNA Sleuthing Tool, but the Battle Over Privacy Looms*, A.B.A. J. (Nov. 1, 2019, 4:20 AM), http://www.abajournal.com/magazine/article/family-tree-genealogy-sites-arm-law-enforcement-with-a-new-branch-of-dna-sleuthing-but-the-battle-over-privacy-looms?ut.

91. *Frequently Asked Questions on CODIS and NDIS*, FBI, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet (last visited Apr. 5, 2020).

The Supreme Court held the collection of DNA from arrestees and direct-match searches of CODIS constitutional in *Maryland v. King*.[92] But the characteristics of direct-match searches the Court focused on in reaching its holding—that the DNA collected did not reveal intimate biological information of source individuals,[93] and that the purpose of direct-matching was identification, rather than criminal investigation[94]—do not apply to genetic genealogy. Rather, genetic genealogy more closely resembles partial-match familial searches of CODIS, an investigative technique only authorized in a handful of states.[95] The Supreme Court has not considered the constitutionality of partial-match familial searching, and it does not fit neatly into traditional Fourth Amendment doctrine. Moreover, the most troubling characteristics of partial-match CODIS searching are further exacerbated in the context of genetic genealogy investigations, and thus must inform the analysis of whether genetic genealogical investigations should be deemed constitutional.

A. Direct-Match Searches Using CODIS

CODIS facilitates searches across the National DNA Index System (NDIS) and state DNA databases for DNA profiles that match suspects' DNA left at a crime scene.[96] NDIS is comprised of multiple databases, including a Convicted Offender or Arrestee Index, and a Forensic Index.[97] CODIS also integrates state indexes, which are separately maintained pursuant to state law, with varying criteria determining when arrestees and/or convicted felons must submit their DNA for inclusion.[98]

CODIS primarily employs a form of DNA typing known as single-tandem repeat (STR) typing, which counts and compares repeat

92. 569 U.S. 435 (2013).

93. *Id.* at 449.

94. *Id.* at 464.

95. James Rainey, *Familial DNA Puts Elusive Killers Behind Bars. But Only 12 States Use It*, NBC NEWS (Apr. 28, 2018, 3:00 AM), https://www.nbcnews.com/news/us-news/familial-dna-puts-elusive-killers-behind-bars-only-12-states-n869711.

96. *Frequently Asked Questions on CODIS and NDIS*, *supra* note 91.

97. *Id.*

98. Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291, 296 (2010); JULIE E. SAMUELS ET AL., URBAN INST., COLLECTING DNA AT ARREST: POLICIES, PRACTICES, AND IMPLICATIONS iii (2013), https://www.ncjrs.gov/pdffiles1/nij/grants/242812.pdf.

sequences at twenty locations,[99] known as "loci," across a genomic strand.[100] Two of these repeat sequences, known as "alleles," are recorded at each locus, yielding forty measurements that comprise the DNA profile stored in NDIS and state databases.[101] All fifty states collect DNA samples and create profiles based on the same twenty loci, so as to be compatible with the CODIS software.[102]

To utilize CODIS in a criminal investigation, law enforcement first submits a forensic sample of the crime scene DNA to a lab in order to create a profile based on the alleles at all twenty loci.[103] Investigators then upload this profile to CODIS, which runs a query against the Offender and Forensic Indexes of every state database and the NDIS, looking for a match.[104] If CODIS returns a match, the law enforcement agency laboratories responsible for creating the queried profile and the database match communicate to confirm the match, share identifying information, and coordinate further investigative steps between the two agencies.[105] A match in a Forensic Index would indicate that there may be a common perpetrator of two separate crimes.[106] A match in an Offender Index would indicate that the offender of a past crime, or a suspect arrested on suspicion of a past crime, deposited DNA at the crime scene currently being investigated.[107] In short, "CODIS sets uniform national standards for DNA matching and then facilitates connections between local law enforcement agencies who can share more specific information about matched STR profiles."[108]

The Supreme Court considered the Fourth Amendment implications of warrantless forensic DNA collection in *Maryland v. King*.[109] The Court held that the mandatory collection of DNA by means of a buccal swab of a suspect's inner cheek, when the suspect

99. From its inception in 1998 until December 31, 2016, CODIS profiles recorded thirteen loci. As of January 1, 2017, CODIS Core Loci now include twenty loci. *Frequently Asked Questi ons on CODIS and NDIS*, *supra* note 91.

100. Murphy, *Relative Doubt*, *supra* note 98, at 295.

101. *Id.*

102. *Id.*

103. *Frequently Asked Questions on CODIS and NDIS*, *supra* note 91.

104. *Id.*

105. *Id.*

106. *Id.*

107. *Id.*

108. Maryland v. King, 569 U.S. 435, 445 (2013).

109. *See id.*

had been arrested for a serious offense supported by probable cause, constituted a reasonable search under the Fourth Amendment.[110] The Court determined a buccal swab of the inner cheek to be a search, as "[v]irtually any 'intrusio[n] into the human body'" will constitute a search under the Fourth Amendment.[111] When analyzing the reasonableness of Maryland's statute, which required the collection of DNA from suspects arrested and charged with a crime or attempted crime of violence or burglary, the Court identified and weighed the government's interests in collecting and databasing arrestee's DNA against the interests of the arrestee, who the Court determined had a diminished expectation of privacy in police custody.[112]

The Court identified five discrete governmental interests. First, it focused on "the need for law enforcement officers in a safe and accurate way to process and identify the persons and possessions they must take into custody."[113] The Court likened the collection of a DNA sample for identification purposes to both fingerprint identification of arrestees and to the comparison of a person's face to a wanted poster of an unidentified suspect.[114] "Finding occurrences of the arrestee's CODIS profile in outstanding cases is consistent with this common practice. It uses a different form of identification than a name or fingerprint, but its function is the same."[115]

Second, the Court recognized the state's interest in identifying the suspect and linking him to past crimes as a means of identifying his propensity for violence and the resulting danger his custody may pose for law enforcement in charge of holding him.[116] Third, the Court pointed to the state's interest in ensuring the suspect shows up for trial and in making decisions regarding his bail, by linking the suspect to past unsolved crimes while still in police custody.[117] Fourth, the Court determined that discovery of past crimes through DNA matching can alert a court of an arrestee's propensity for violence that could pose a

110. *Id.* at 465–66.

111. *Id.* at 446 (second alteration in original) (quoting Schmerber v. California, 384 U.S. 757, 770 (1966)).

112. *Id.* at 461–62.

113. *Id.* at 449.

114. *Id.* at 445, 451–52.

115. *Id.* at 452.

116. *Id.*

117. *Id.* at 453.

danger to the public, further informing bail determinations.[118] Last, the Court noted that connecting an arrestee with a past crime may "have the salutary effect of freeing a person wrongfully imprisoned for the same offense."[119]

The Court weighed these interests against the "degree to which the search invades an [arrestee's] legitimate expectations of privacy."[120] It looked at both the invasiveness of the inner cheek buccal swab, which it determined was a negligible intrusion,[121] and an arrestee's diminished expectation of privacy.[122] The Court emphasized that "the necessary predicate of a valid arrest for a serious offense is fundamental."[123] Thus, the Court held that the taking of DNA by buccal swab from an arrestee with a diminished expectation of privacy was "[a] brief intrusion . . . subject to the Fourth Amendment, but a swab of this nature [did] not increase the indignity already attendant to normal incidents of arrest," and was therefore reasonable when weighed against the significant government interests previously identified.[124]

The Court deemed the initial collection of the DNA sample to be the search that triggered the Fourth Amendment, and hastily dismissed the implications of law enforcement's analysis and conversion of the sample into a profile that could then be searched across all CODIS-linked databases *after* the DNA was collected.[125] The Court reasoned that "the processing of respondent's DNA sample's 13 CODIS loci did not intrude on respondent's privacy in a way that would make his DNA identification unconstitutional"[126] because the genetic information recorded at these loci does not code for specific proteins capable of revealing hereditary traits but rather can only be used for identification purposes; the Court labeled this genetic information "junk."[127] Importantly, the Court emphasized that "[i]f in the future police analyze samples to determine, for instance, an arrestee's

118. *Id.*
119. *Id.* at 455.
120. *Id.* at 461.
121. *Id.* at 446.
122. *Id.* at 462.
123. *Id.* at 461
124. *Id.* at 464.
125. *See id.* at 464–65.
126. *Id.* at 464.
127. *Id.* at 445.

predisposition for a particular disease or other hereditary factors not relevant to identity, that case would present additional privacy concerns not present here."[128]

Because the DNA analysis revealed no personal medical or hereditary information, and the CODIS search was likened to a search of fingerprint records for purely identification purposes, the *King* Court found such searches constitutional even in the absence of individualized suspicion and a warrant. In reaching this conclusion, however, the Court completely ignored the purpose for which CODIS searches are most often performed: to find and identify suspects of unsolved crimes.[129] Justice Scalia, in dissent, repeatedly stressed the Maryland statute's true purpose—ordinary criminal investigation and evidence-gathering—which he argued is always prohibited by the Fourth Amendment absent individualized suspicion.[130] He argued that a reasonableness inquiry should only be undertaken if the suspicionless search was performed for a government purpose other than solving crimes, under the special needs doctrine.[131] "No matter the degree of invasiveness, suspicionless searches are *never* allowed if their principal end is ordinary crime-solving."[132] Because the arrestee's DNA would be searched against a database of forensic DNA from unsolved crimes for which he was not a suspect, Justice Scalia argued, such a search should be prohibited by the Fourth Amendment without a warrant.[133] Scalia warned in dissent that the ramifications of the majority's decision would be that "your DNA can be taken and entered into a national DNA database if you are ever arrested, rightly or wrongly, and for whatever reason."[134] The Court did not address this fear, however, instead accepting the argument that the primary

128. *Id.* at 464–65.
129. *Id.* at 474–75 (Scalia, J., dissenting).
130. *Id.* at 466.
131. *Id.* at 468.
132. *Id.* at 469 (emphasis in original).
133. *Id.* at 480–81.
134. *Id.* at 481. While widespread collection of DNA by law enforcement for minor crimes has not come to pass in the ensuing six years since *King*, the rapid increase of commercial genealogy databases in criminal investigations, the extremely wide net such searches can cast, and the detailed information such databases provide, are creating an ad hoc national database by association that, combined with law enforcement's use of genealogical investigative techniques, may become even more potent than the national DNA database Scalia feared.

purpose of CODIS was identification, rather than criminal investigation and thus finding it constitutional.

B. Partial Match Familial Searching

While direct-match searches utilizing CODIS are widespread and common throughout all fifty states and various federal law enforcement agencies, partial-match familial DNA searching (FDS) is far rarer and more controversial. A CODIS query can be set to high, medium, or low stringency, determining how many loci must match for the system to yield a "matching" profile.[135] A high level stringency query requires all twenty loci to match, indicating the unidentified DNA sample originated from the same person whose profile the CODIS query returned. But moderate and low level stringency queries will return profile results that only match some of the loci, indicating that the person from whom the unidentified DNA originated is a relative of the CODIS DNA profile that the query returned.[136] But the CODIS software is not designed for FDS, and it fails to take into account that certain combinations of genetic information on certain alleles at each loci are more common in the general population than others.[137] As a result, some states have developed software for intentional familial searching that further analyzes partial matches to determine the probabilities that certain allelic matches indicate familial relationships, based upon their relative scarcity in the general public.[138] Matches of common allelic combinations have a lower chance of indicating familial relationships than matches of rarer combinations.[139]

Twelve states explicitly allow FDS by law enforcement,[140] while six states explicitly prohibit it.[141] Maryland and the District of

135. SARA DEBUS-SHERRILL & MICHAEL B. FIELD, NAT'L CRIMINAL JUSTICE REFERENCE SERV., UNDERSTANDING FAMILIAL DNA SEARCHING: POLICIES, PROCEDURES AND POTENTIAL IMPACT 3 (2017), https://www.ncjrs.gov/pdffiles1/nij/grants/251043.pdf.

136. *Id.*

137. Murphy, *Relative Doubt*, *supra* note 98, at 300.

138. *Id.* at 302–03.

139. *Id.* at 295, 343–44.

140. Arizona, California, Colorado, Florida, Minnesota, New York, Ohio, Texas, Utah, Virginia, Wisconsin, and Wyoming. Illinois and Louisiana are currently considering legislation. Rainey, *supra* note 95.

141. Murphy, *Relative Doubt*, *supra* note 98, at 302; Natalie Ram, *Incidental Informants: Police Can Use Genealogy Databases to Help Identify Criminal Relatives—but Should They?*, MD. B. J., July–Aug. 2018, at 8, 11–12.

Columbia have enacted statutes banning the practice, and the rest do so through regulations or law enforcement policy.[142] The remaining states take a more flexible non-statutory approach, often allowing "unintentional" partial match reporting but not intentional familial searching, a distinction some have criticized as a merely rhetorical attempt to allow the practice while avoiding public criticism and controversy.[143] While the FBI does not allow familial searching of NDIS, it does allow moderate stringency searches, which can be effective in finding matches to forensic samples that contain more than one person's DNA.[144]

Although the constitutionality of familial DNA searching has been widely debated, it has yet to be decided by courts. Nationally, FDS is quite uncommon.[145] California, for example, explicitly allows it, yet when cases that utilized FDS to generate leads have gone to trial there, prosecutors generally have not introduced the results of these searches into evidence, and defense attorneys have not challenged the legality of the practice.[146] A recent case study of FDS policies in California noted:

> Interviewees[147] generally expressed confidence that an FDS case would be treated like a regular CODIS DNA match case and that the use of FDS would not likely be raised in court. Interviewees explained that FDS is just another investigative tool for law enforcement and, as with any other tool, is not explicitly brought up in court unless the defense raises it as an issue (most likely during pre-trial motions). Interviewees also argued that FDS cases are no different than any other case dealing with DNA and do not raise any unique 4th

142. Murphy, *Relative Doubt*, *supra* note 98, at 302; Ram, *supra* note 141, at 11.

143. Murphy, *Relative Doubt*, *supra* note 98, at 341.

144. *Frequently Asked Questions on CODIS and NDIS*, *supra* note 91.

145. *See* Rainey, *supra* note 95 ("The practice remains so uncommon that experts aren't sure how many detectives and prosecutors are even aware DNA can provide an indirect pathway to suspects.").

146. MICHAEL B. FIELD ET AL., NAT'L CRIMINAL JUSTICE REFERENCE SERV., STUDY OF FAMILIAL DNA SEARCHING: POLICIES AND PRACTICES 19, 21 (2017), https://www.ncjrs.gov/pdffiles1/nij/grants/251081.pdf.

147. Eighteen stakeholders were interviewed in California, encompassing representatives of state and local crime labs, the police, prosecutors, the judiciary, a civil liberties attorney, a victim's advocate and policy staff. *Id.* at 2.

> Amendment questions compared to traditional DNA cases.[148]

And yet the constitutionality of familial DNA searching has been widely debated by legal scholars. The shared nature of DNA between genetic relatives causes familial DNA searches to "frustrate ordinary principles of Fourth Amendment analysis."[149] There tends to be agreement amongst scholars that FDS would likely be permissible under traditional Fourth Amendment doctrine, but perhaps only because "familial searches fall between the cracks of a range of uncertain constitutional doctrines with regard to even the most preliminary question of whether the Fourth Amendment applies."[150]

First, there is the unclear preliminary question of whose privacy interests would be violated in an FDS case—the databased arrestee, his or her relatives, or both.[151] The source of an indexed DNA profile, an arrestee, could not assert a Fourth Amendment challenge, as the arrestee would have been lawfully profiled and indexed under *King*, based on the arrestee's diminished expectation of privacy.[152] Moreover, querying the CODIS-linked databases for the purpose of identification was held not to be a search subject to the Fourth Amendment by the *King* Court, despite the issue being given relatively little attention by the majority and vigorously opposed by the dissent.[153] Indeed, the Supreme Court has never considered a database query to be a constitutional event.[154]

Assessing the Fourth Amendment interests of the relatives of the databased individual is more difficult. Unlike an offender whose DNA profile was collected while in custody and subsequently searched by CODIS, the offender's relatives' expectation of privacy is not diminished due to an arrest. The overlap of their DNA with that of their offender-relative is the result of "biology, not choice. Indeed, genetic ties are both involuntary and immutable. They cannot be

148. *Id.* at 19.
149. Ram, *supra* note 141, at 10.
150. Murphy, *Relative Doubt*, *supra* note 98, at 334.
151. *Id.* at 334–35.
152. *See* Maryland v. King, 569 U.S. 435, 464–65 (2013).
153. *See generally id.* at 464–82 (majority opinion and Scalia, J., dissenting).
154. *See* Emily Berman, *When Database Queries Are Fourth Amendment Searches*, 102 MINN. L. REV. 577, 603–04 (2017).

controlled or escaped."[155] It is unclear, however, if such relatives even have a privacy interest being infringed.[156] The profile used to conduct the CODIS search is not derived from their cells.[157] Further, it is unclear what harm, if any, these relatives suffer, and whether such harm results from a violation of their Fourth Amendment rights.[158] Because the genetic information stored in CODIS databases is comprised of identifying "junk" only, FDS does not implicate information nearly as intimately personal as does genetic genealogy investigations. And because FDS cannot identify relatives as far removed as GEDmatch can, these investigations do not involve trained genealogists constructing extensive family trees. Accordingly, FDS is significantly less intrusive than genetic genealogy. Thus, it is difficult to imagine what injury the relatives of databased individuals might suffer. Simply casting temporary suspicion on these individuals, absent more, is unlikely to be deemed intrusive enough to trigger Fourth Amendment protections.

Nevertheless, some argue familial DNA searches should be prohibited because "they embody the very presumptions that our constitutional and evidentiary rules have long endeavored to counteract: guilt by association, racial discrimination, propensity, and even biological determinism."[159] Professor Erin Murphy argues the constitutional focus should be on the use and further searching of lawfully collected DNA samples, rather than on the initial collection of the sample.[160] Murphy has articulated one such hypothetical view a court could take to find a familial DNA search to violate the Fourth Amendment:

> The partial match search itself constitutes the unauthorized act. Its unreasonableness would hinge upon the arbitrariness of casting suspicion on offender relatives, as well as the impermissibility of exploiting databases compiled on the premise of lessened privacy of offenders to access the fully protected DNA profiles of relatives. . . . In stark terms: the partial match search, and the inference drawn from the match itself, invoke constitutional scrutiny because they intrude on

155. Ram, *supra* note 141, at 11.
156. *Id.*
157. *Id.*
158. Murphy, *Relative Doubt*, *supra* note 98, at 334.
159. *Id.* at 304.
160. *Id.* at 335–36.

> the legitimate expectation of privacy held by the relative in her half of the offender's genetic code, and are impermissible because they do so without individualized or particularized suspicion. The rationale justifying such warrantless, suspicionless searches in the case of a direct match—namely, the diminished expectation of privacy and recidivist threat of convicted offenders—is absent when it comes to relatives, who retain the full force of Fourth Amendment protection.[161]

Not all agree with Professor Murphy's formulation, however. Rather, FDS could be framed as nothing more than a comparison between a forensic sample and a lawfully obtained DNA profile, with the result—that most loci match but a few do not—reported to law enforcement investigators by their lab technicians.[162] The inference that such a result indicates kinship, and any subsequent investigation of leads utilizing common and uncontroversial techniques, would not implicate the Fourth Amendment.[163] Absent a violation of a databased individual's relative's Fourth Amendment rights, which the Supreme Court has held to be "personal,"[164] that relative would have no recourse to address harm caused by the dissemination of intimate information inferred from the databased individual's shared genetic information.[165] While courts have yet to weigh in, the view generally shared by both prosecutors and defendants in the small handful of cases utilizing the technique that have actually gone to trial, as well as some legal scholars, is that the Fourth Amendment currently does not prohibit familial DNA searching.[166]

161. *Id.* at 336–37.

162. *See, e.g.*, Jules Epstein, "*Genetic Surveillance"—The* Bogeyman *Response to Familial DNA Investigations*, 2009 U. ILL. J.L. TECH. & POL'Y 141, 161.

163. *Id.* at 161–62.

164. Rakas v. Illinois, 439 U.S. 128, 133–34 (1978).

165. Epstein, *supra* note 162, at 161–62.

166. *Id.* at 165; *see also* FIELD ET AL., *supra* note 146, at 21.

IV. COMMERCIAL GENETIC GENEALOGY IN CRIMINAL INVESTIGATIONS AND THE FOURTH AMENDMENT

A. Fourth Amendment Analysis Before Carpenter

1. Does a Commercial Genetic Genealogical Investigation Constitute a Search?

Fourth Amendment analysis of warrantless commercial genetic genealogy investigations by law enforcement is in many ways akin to the analysis of FDS—it similarly "frustrate[s] ordinary principles of Fourth Amendment analysis."[167] However, a stronger argument can be made that genetic genealogy investigations trigger Fourth Amendment protections because of the more revealing nature of the genetic information at issue. The Fourth Amendment protects against "unreasonable searches and seizures" of one's "person[], house[], papers, and effects."[168] Prior to the Supreme Court's decision in *Katz v. United States*,[169] a trespass upon one's real property or personal possessions was generally required to constitute a search.[170] The Court abandoned such an approach in *Katz*, declaring that the "Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures" and that "the 'trespass' doctrine . . . can no longer be regarded as controlling."[171] In finding the government's uninvited electronic eavesdropping of a conversation Katz was having in a public phone booth to be a violation of his Fourth Amendment rights, the Court established an alternate test to determine the existence of a protected interest: whether an individual had "exhibited an actual (subjective) expectation of privacy . . . that society is prepared to recognize as 'reasonable.'"[172]

There are three primary steps that comprise a genetic genealogy investigation, each of which may implicate the Fourth Amendment: (1) the creation of the database by uploading genetic samples for analysis and storage as genetic profiles in the database; (2) running a forensic sample acquired from the crime scene through the database

167. Ram, *supra* note 141, at 10.

168. U.S. CONST. amend. IV.

169. 389 U.S. 347 (1967).

170. *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding surveillance not prohibited by the Fourth Amendment absent any trespass or seizure of material object), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

171. *Katz*, 389 U.S. at 353.

172. *Id.* at 361 (Harlan, J., concurring).

to find relatives, as far out as third cousins, amongst the database's users; and (3) the genealogical research and building of family trees, tracing backward from the users' profiles identified by the database query in step two to a common ancestor, and then forward from that ancestor to identify potential suspects in the crime being investigated.

Because the government did not mandate the collection of the genetic samples used to create the profiles that comprise commercial databases, there would be no Fourth Amendment event at the point of collection (step one) as there would be with new CODIS profile entries, ruled a constitutional search in *King*.[173] Law enforcement is not involved in the collection or analysis of any new user's genetic sample, nor the derivation of the genetic information from the sample that allows for the creation of the profile, so the creation of the database and the addition of new profiles therein would not constitute a search.

Steps two and three, however, are potentially Fourth Amendment events. Putting aside for a moment that the users of the database uploaded their DNA profiles willingly—would the accessing of DNA profiles already stored in a commercial DNA database, and the comparison of those profiles against a forensic sample by law enforcement, constitute a search under traditional Fourth Amendment doctrine? And would the extensive research through public records, the press, social media and more, necessary to build the family tree, constitute its own search, when all such records are public?

The Supreme Court has held the testing of biological samples that reveal intimate details about the source to be a search independent of the collection of the sample.[174] The Court has declared that one has an expectation of privacy in confidential information such as private genetic and medical information, taking into consideration the sensitivity of information that can be derived from biological samples,[175] and has stated that such "intrusions must be deemed searches under the Fourth Amendment."[176] And while the Court in *King* held that the analysis of the respondent's DNA was not an

173. Maryland v. King, 569 U.S. 435, 465 (2013).

174. Murphy, *Relative Doubt*, *supra* note 98, at 335.

175. Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 616–17 (1989) ("It is not disputed, however, that chemical analysis of urine, like that of blood, can reveal a host of private medical facts about an employee, including whether he or she is epileptic, pregnant, or diabetic.").

176. *Id.* at 617.

unconstitutional intrusion on his privacy, the Court premised its holding on the fact that the thirteen CODIS loci were noncoding "junk" that revealed no personal information other than identification.[177] The Court's reasoning thus indicates that an individual *could* have a protected expectation of privacy in their genetic information if personal information were to be revealed.[178] The genetic information being accessed by law enforcement here is far more revealing than "junk" DNA. It seems to follow, then, that one has a reasonable expectation of privacy in their genetic information contained in the records of a commercial genetic genealogy database such as GEDmatch.

But when law enforcement begins an investigation utilizing GEDmatch, it is not collecting and analyzing the samples contained therein, only the cold case sample found at the crime scene. Rather, they are searching a database that *already* contains such profiles, created by the sources of the samples themselves. So courts would likely follow *King* and determine that running a sample through GEDmatch is no different than fingerprint identification, and thus not a search.[179] Indeed, lower courts have held that accessing DNA profile records using CODIS is not a Fourth Amendment search.[180] And the Supreme Court has never treated database queries generally as Fourth Amendment events.[181] In cases involving databases, the Court has limited its discussion to either: (a) the constitutionality of the collection of the information contained therein;[182] (b) the adequacy of statutory safeguards and rules governing disclosure of information;[183] or (c) whether law enforcement reliance on mistaken database entries

177. *King*, 569 U.S. at 464–65.

178. *See id.* at 464.

179. *Id.* at 451–52.

180. *See, e.g.*, Johnson v. Quander, 440 F.3d 489, 498 (D.C. Cir. 2006) ("We conclude that accessing the records stored in the CODIS database is not a 'search' for Fourth Amendment purposes. As the Supreme Court has held, the process of matching one piece of personal information against government records does not implicate the Fourth Amendment.").

181. Berman, *supra* note 154, at 604.

182. *See, e.g.*, *King*, 569 U.S. at 464 (holding collection of DNA from arrestees using buccal swab constitutional).

183. *See generally* Erin Murphy, *Databases, Doctrine, and Constitutional Criminal Procedure*, 37 FORDHAM URB. L.J. 803, 811–17 (2010) (discussing Smith v. Doe, 538 U.S. 84 (2003), U.S. Dept. of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749 (1989), and Whalen v. Row, 429 U.S. 589 (1977)).

should trigger the exclusionary rule.[184] Indeed, it is widely accepted that "the [F]ourth [A]mendment does not control how properly collected information is deployed."[185] Thus, it is unlikely courts would find step two, in isolation, to be a search solely because the information being accessed is more intimate than fingerprint records or "junk" DNA.

The third step in a genetic genealogy investigation, the genealogical research and the building of the family tree, is unlikely to be considered a search when viewed in isolation either. Many of the genealogists that law enforcement agencies have hired to perform this step developed their skills conducting genealogy research as a hobby, helping adopted children find birth parents.[186] Using publicly available information to follow leads and draw inferences is standard, uncontroversial detective work, and it would be difficult to argue that society does not expect law enforcement to conduct such investigations, or considers such investigations unreasonable.

But a plausible argument can be made that when considering the investigatory technique as a whole—combining genetic information obtained through a GEDmatch query with a genealogist's research to draw a host of inferences—a Fourth Amendment search has occurred. The Supreme Court acknowledged, in *United States v. Jones*,[187] that discrete actions by law enforcement that would not rise to the level of a search in isolation could, in the aggregate, constitute a search,[188] often referred to as the mosaic theory. Although the majority's holding in *Jones*—that the use of a GPS device attached to the defendant's car to track his movements for twenty-eight days constituted a search—was based on a traditional trespass theory, five Justices also determined a search occurred based on the defendant's reasonable expectation of privacy.[189] This conclusion was not based on a

184. *Id.* at 817–21 (discussing Herring v. United States, 555 U.S. 135 (2009) and Arizona v. Evans, 514 U.S. 1 (1995)).

185. Berman, *supra* note 154, at 604 (alteration in original) (citing Green v. Berge, 354 F.3d 675, 689 (7th Cir. 2004)); *see also* Murphy, *Databases, Doctrine, and Constitutional Criminal Procedure*, *supra* note 183, at 821 ("As shown, the Supreme Court has paid scant (and inconsistent) heed to the peculiar features of databasing or to what special concerns might inform the investigations conducted or evidence collected from them.").

186. Murphy, *She Helped Crack the Golden State Killer Case*, *supra* note 10.

187. 565 U.S. 400 (2012).

188. *See id.* at 430 (Alito, J., concurring).

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

determination that a person has a reasonable expectation of privacy in any single specific movement, or even in their movements over a short term, as one's movements usually occur in public spaces.[190] Rather, it was based on the effect of combining many discrete location data points to create a long-term surveillance of one's movements that could, when combined with other information, allow inferences to be drawn regarding "familial, political, professional, religious, and sexual associations."[191] Combining long-term GPS tracking with additional publicly available information to make inferences resulted in "the Government's unrestrained power to assemble data that reveal private aspects of identity [that] is susceptible to abuse."[192]

Genetic genealogy investigations are no different in this regard. Erin Murphy's argument that FDS is a Fourth Amendment search—that "the partial match search, and the inference drawn from the match itself, invoke constitutional scrutiny because they intrude on the legitimate expectation of privacy held by the relative in her half of the offender's genetic code"[193]—is stronger in the context of genetic genealogy investigations. This is because genetic genealogy profiles reveal far more intimate information than the identifying "junk" DNA that comprises the profiles in CODIS databases. In genetic genealogy investigations, law enforcement learns not only that kinship exists, but how closely and on which side of the family, and it can draw inferences about biological characteristics of members of the family tree based upon the genetic information in the database profiles.[194]

Because it is unlikely that either step two, the database query, or step three, the genealogical investigation, would constitute a search when viewed in isolation, the potential Fourth Amendment search considered in the following sections will be the overall investigative technique, combining these two steps into one action that may constitute a search. Further, this search can run against two classes of people: the patrons of the genetic genealogy database being queried, and the family members of any "hits" that a query returns, who are then investigated in the course of building the family tree, including the suspect ultimately identified by the investigation.

190. *Id.* at 416.
191. *Id.* at 415.
192. *Id.* at 416.
193. Murphy, *Relative Doubt*, *supra* note 98, at 337.
194. Murphy, *How an Unlikely Family History Website Transformed Cold Case Investigations*, *supra* note 33.

2. Third-Party Doctrine Before *Carpenter*

Because the genetic information stored by a commercial genetic genealogy database was submitted voluntarily by its users, and the subsequent genealogical research is comprised entirely of publicly available records and information, a genetic genealogy investigation that might otherwise be considered a search would not implicate the Fourth Amendment under the third-party doctrine. Under the third-party doctrine, articulated by the Supreme Court in *United States v. Miller*[195] and *Smith v. Maryland*,[196] "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[197] A commercial database's users, therefore, like those whose DNA was collected pursuant to an arrest, lack a reasonable expectation of privacy in the genetic information they have voluntarily submitted to the database, so law enforcement access of these records would not constitute a search.

As with FDS, the analysis is less clear when determining whether a database user's relatives have a reasonable expectation of privacy in their DNA that they share with the user, and whether that expectation of privacy has been intruded upon by investigators. The commercial database does not actually contain the personal genetic information of intermediary relatives on the family tree in between the forensic source DNA and the source's relatives who have uploaded their DNA to the database. The database query only produces a record of how closely the source of the forensic DNA and certain database users are related and on which branch of their lineage, based on the overlapping of long stretches of autosomal DNA markers.[198] Any intimate information revealed by the database search pertains directly only to the users, who relinquished any reasonable expectation of privacy in such information under the third-party doctrine, and the source of the forensic sample. Accurate assumptions regarding intermediary relatives' biological characteristics can be inferred based on their location on a lineage between the database user and the forensic source, but there is not actually a genetic search conducted of any intermediary relatives.

195. 425 U.S. 435 (1976).
196. 442 U.S. 735 (1979).
197. *Id.* at 743–44.
198. *How Genetic Genealogy Works*, *supra* note 45.

In the aggregate, however, genetic genealogical investigations delve very deeply into the intimate personal details of many relatives of the forensic source sample, potentially revealing if an individual "was born out of wedlock, was the product of incest, or carries genetic diseases."[199] It is certainly reasonable to expect such information to be free from government surveillance. The depth and breadth of intimate personal information at issue, and the speed and efficiency with which modern technology allows law enforcement to discover and compile such information, suggest the traditional third-party doctrine should not apply. As genetic genealogical investigations rapidly become faster and more efficient, they are beginning to function more akin to a national genetic database.[200] The public's unease with GEDmatch violating its terms of service to allow law enforcement access to investigate an assault in real time clearly demonstrates the need for a different approach. The Supreme Court's recent decision in *United States v. Carpenter* establishes one such approach to extending Fourth Amendment protection to certain types of information and surveillance technologies in the digital age and lays the foundation for further extensions.

B. Fourth Amendment Analysis After Carpenter

1. *Carpenter v. United States*

The Supreme Court in *Carpenter v. United States* upended traditional third-party doctrine, recognizing that the rapid development of modern technologies, especially information technologies, has resulted in the production and storage of extensive, easily searchable, and highly revealing records by third parties. Timothy Carpenter had been convicted of multiple armed robberies of several Radio Shack and T-Mobile stores.[201] To prove Carpenter's presence at each robbery, prosecutors introduced as evidence 127 days of cell-site location information (CSLI), which they acquired from

199. Murphy, *Genealogy Sites Have Helped Identify Suspects*, *supra* note 88.

200. *See* Yaniv Erlich et al., *Identity Inference of Genomic Data Using Long-Range Familial Searches*, 362 SCI. 690, 690 (Nov. 9, 2018), https://science.sciencemag.org/content/sci/362/6415/690.full.pdf (predicting 99 percent of Caucasian Americans of Northern European descent will be identifiable through genetic genealogy in the near future).

201. Carpenter v. United States, 138 S. Ct. 2206, 2212–13 (2018).

Carpenter's cellular service provider pursuant to a request under the Stored Communications Act, rather than a warrant.[202] Carpenter challenged the admission of the CSLI evidence, arguing a warrant was required to obtain it.[203] The Supreme Court agreed.[204]

The Court claimed its holding to be a narrow one, simply declining to extend the third-party doctrine as established in *Smith* and *Miller* to CSLI, because CSLI reveals a "detailed chronicle of a person's physical presence compiled every day, every moment, over several years. Such a chronicle implicates privacy concerns far beyond those considered in *Smith* and *Miller*."[205] But the Court went significantly further, recognizing that "technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes,"[206] and continuing a line of reasoning introduced in *Kyllo v. United States*,[207] and continued in *Riley v. California*,[208] that sought to "preserv[e] . . . that degree of privacy against government that existed when the Fourth Amendment was adopted."[209]

The Court in *Kyllo* held that law enforcement's use of a thermal imager to detect heat consistent with marijuana cultivation emanating from the defendant's home was a search requiring a warrant, even though investigators never entered the home.[210] The Court explained

> that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," constitutes a search—at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.[211]

In *Riley*, the Court based its holding—that law enforcement needed a warrant to search the contents of a cell phone incident to

202. *Id.*
203. *Id.*
204. *Id.* at 2223.
205. *Id.* at 2220.
206. *Id.* at 2214.
207. 533 U.S. 27 (2001).
208. 573 U.S. 373 (2014).
209. *Carpenter*, 138 S. Ct. at 2214 (quoting *Kyllo*, 533 U.S. at 34).
210. *Kyllo*, 533 U.S. at 34.
211. *Id.* at 34–35 (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

lawful arrest—on a recognition that cell phones contain information that is not only quantitatively much greater but qualitatively different than what might be traditionally on an arrestee's person at the time of arrest.[212] Because cell phones collect "many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record," because their storage capacity allows them to retain information stretching back to when the phone was first acquired, and because of the pervasiveness of cell phones in modern life, the Court recognized the implications of modern technology on privacy in the information age.[213]

The Court's reasoning in *Carpenter* is a direct continuation of *Kyllo* and *Riley*. By combining its concern for the potential for "seismic shifts in digital technology" to erode Fourth Amendment privacy interests recognized since the founding, with its well-established recognition that "individuals have a reasonable expectation of privacy in the whole of their physical movements,"[214] the Court determined that not all information is the same, and one has not automatically lost all expectation of privacy in certain types of information just because it is retained by a third party.[215]

2. The *Carpenter* Criteria

In finding CSLI to be a distinct category of information, the Court recognized three characteristics that distinguished it from more traditional types of information generally subject to the third-party doctrine. In so doing, the Court established criteria that can be applied to determine whether other types of digital information might be similar in nature and thus excepted from third-party doctrine. These criteria have provided some guidance to lower courts when determining whether to extend *Carpenter's* holding to other fact-patterns.[216]

212. *Riley*, 573 U.S. at 393.

213. *Id.* at 394.

214. *Carpenter*, 138 S. Ct. at 2219, 2217.

215. *Id.* at 2219 ("The Government thus is not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information.").

216. *See* Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 527 (7th Cir. 2018).

First, the information in question must be of a "deeply revealing nature."[217] Like GPS surveillance, or the contents of a cell phone, CSLI "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, religious, and sexual associations.' These location records 'hold for many Americans "the privacies of life."'"[218]

Second, the information must be of a certain "depth, breadth, and comprehensive reach."[219] The Court focused on the common practice of individuals carrying their cell phones at all times, likening them to ankle monitors that can "achieve[] near perfect surveillance."[220] The Court also focused on "the retrospective quality of the data," explaining that when the Government decides to acquire a person's CSLI records, it "can now travel back in time to retrace a person's whereabouts," and is only limited by the policies of cellular providers governing how long they retain such records.[221] Further, because of its retrospective nature, "police need not even know in advance whether they want to follow a particular individual, or when."[222]

Paul Ohm has explained this factor as follows:

> *Depth* refers to the detail and precision of the information stored. . . . In contrast, *breadth* refers to time in two ways: how frequently the data is [sic] collected, and for how long the data has [sic] been recorded. . . . Finally, *comprehensive reach* refers to the number of people tracked in the database.[223]

He argues that this factor reflects the Court's embrace and revival of the mosaic theory, first articulated by the Court in *Jones*, which recognizes that while a particular instance of short-term surveillance may not amount to a search in isolation, many such instances in the aggregate can reveal not only quantitatively more information, but a

217. *See Carpenter*, 138 S. Ct. at 2223.
218. *Id.* at 2217 (citations omitted).
219. *See id.* at 2223.
220. *Id.* at 2218.
221. *Id.*
222. *Id.*
223. Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 372–73 (2019) (emphasis in original).

qualitatively different and more intimate kind of information, and thus would constitute a search.[224]

Last, the collection of the information must be "automatic."[225] The Court noted that CSLI is "continually logged for all of the 400 million devices in the United States," and because cell phones are such an integral and pervasive part of life, "[o]nly the few without cell phones could escape this tireless and absolute surveillance."[226]

Legal scholars have articulated the criteria for applying *Carpenter* to other types of digital information in varying ways, formulating somewhat different tests and emphasizing certain criteria over others. Paul Ohm articulates three factors derived directly from the text of *Carpenter* to determine whether the information: "(1) has a deeply revealing nature; (2) possesses depth, breadth, and comprehensive reach; and (3) results from an inescapable and automatic form of data collection."[227] He posits that to satisfy the third factor, the data collection must be inescapable because it is a byproduct of "services one needs to use to be a functioning member of today's society," and automatic because users of the service cannot refuse the data collection without forgoing use of the product or service.[228]

Susan Freiwald and Stephen Smith articulate a variation on similar factors.[229] Their test analyzes "whether the technique was (1) *hidden*, (2) *continuous*, (3) *indiscriminate*, and (4) *intrusive*."[230] Their first factor, whether the technique is hidden, reflects the Court's concern that society would not reasonably expect law enforcement to be secretly monitoring and recording every single person's movements over an extended period of time.[231] In essence, this factor embodies the traditional *Katz* reasonable-expectation-of-privacy test. The second factor, whether the technique is continuous, reflects the Court's concern with retrospectivity.[232] The third factor, whether the

224. *Id.* at 373.
225. *See Carpenter*, 138 S. Ct. at 2223.
226. *Id.* at 2218.
227. Ohm, *supra* note 223, at 378.
228. *Id.* at 376–77.
229. *See* Susan Freiwald & Stephen Wm. Smith, *The* Carpenter *Chronicle: A Near Perfect Surveillance*, 132 HARV. L. REV. 205, 219 (2018).
230. *Id.* (emphasis in original).
231. *Id.*
232. *Id.* at 220.

technique is indiscriminate, looks at the pervasiveness of the information collection, and whether it "poses the danger of government fishing expeditions through databases," reflecting the Founders' fear of general warrants.[233] The fourth factor, intrusiveness, is the equivalent of Paul Ohm's "deeply revealing nature" factor, and they similarly add "expense and efficiency" as a factor as well.[234]

Orin Kerr articulates a different test for applying *Carpenter*, based on his theory of equilibrium-adjustment, which argues that "[w]hen technology expands government power in a transformative way, courts change the Fourth Amendment rules to restore preexisting limits on that power."[235] This practice is evident in the Supreme Court's reasoning in *Kyllo*[236] and *Riley*.[237] Kerr argues that after *Carpenter*, what triggers a search is not actually the content of the information law enforcement acquires, but whether, because of a "broader technological shift," law enforcement can access today records it could not access traditionally.[238] "When technology enables surveillance that could not occur before, the new surveillance becomes a search. To avoid a dramatic increase in government power, the new surveillance tools that digital technology creates are to be slotted into the legal box of searches that require a warrant."[239]

---

233. *Id.*

234. *See id*; *see also* Ohm, *supra* note 223, at 378.

235. ORIN S. KERR, THE DIGITAL FOURTH AMENDMENT, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301257 (forthcoming) (manuscript at 8) (December 19, 2018 draft).

236. In *Kyllo*, the Supreme Court noted,

> [O]btaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," constitutes a search—at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.

Kyllo v. United States, 533 U.S. 27, 34 (2001) (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

237. In *Riley*, the Supreme Court noted,

> Today, by contrast, it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate. Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.

Riley v. California, 573 U.S. 373, 395 (2014) (citation omitted).

238. KERR, *supra* note 235 (manuscript at 10).

239. *Id.*

Kerr identifies three requirements for *Carpenter* to apply to a particular type of record, thus necessitating a warrant for that record to be searched, regardless of whether it is held by a third party. First, "[t]he records must be of a kind and nature that generally could not be collected in a pre-digital age."[240] Traditional records are still subject to the traditional third-party doctrine, as the Court makes clear in its holding.[241] Second, the records must have been "created without the subject's meaningful voluntary choice," or "inescapably . . . through use of broadly-used services."[242] Last, the records must "reveal an intimate portrait of a person's life typically beyond legitimate state interest."[243] According to Kerr, any information satisfying these three criteria is subject to *Carpenter* protection, and the use by law enforcement of "a digital technology . . . that was unavailable before the digital age" to access such information is a search.[244]

3. Does *Carpenter* Protect Genetic Genealogy Information?

It is unlikely *Carpenter* affords Fourth Amendment protection to information obtained from genetic genealogy investigations. The information is clearly of a "deeply revealing nature." It likely also satisfies the "depth, breadth, and comprehensiveness" criterion. However, the collection of the information by the database is not "inescapable and automatic," at least as pertains to the database user. This deficiency would most likely prove fatal, precluding extension of *Carpenter* to genetic genealogy database information, absent a generous extension of the underlying policy concerns that led the Court to its decision.

a. Deeply revealing nature

The information contained in genetic genealogy profiles, and the information that can be gleaned from subsequent genealogical research and attendant inferences, is easily as intimate as CSLI data, if not more so. The Court in *Carpenter* was concerned about CSLI data because of the intimate details of a person's life that could be

240. *Id.* (manuscript at 16).
241. *See* Carpenter v. United States, 138 S. Ct. 2206, 2216–17 (2018).
242. KERR, *supra* note 235 (manuscript at 20).
243. *Id.* (manuscript at 22).
244. *Id.* (manuscript at 40).

learned by combining a record of a person's location over time with other available information, and drawing inferences.[245] Those inferences could reveal "familial, political, professional, religious, and sexual associations."[246]

Here, by combining the wealth of genetic information contained in the genetic profiles of a GEDmatch user and a related forensic sample, with knowledge regarding the user's degree of kinship with his or her intermediary relatives on the family tree between the two, law enforcement can glean deeply revealing information about the entire familial line, including "predisposition for a particular disease or other hereditary factors not relevant to identity."[247] Concerns raised about the sensitivity of information that might be disclosed through FDS, such as "abandoned parental bonds, adoptee relationships, children conceived through technology, even family secrets about paternal identity,"[248] are even more pressing in the context of a database like GEDmatch, where the genetic information stored is so much more detailed.[249]

b. Breadth, depth and comprehensiveness

Genetic genealogy information likely also satisfies the "depth, breadth, and comprehensive reach" requirement for *Carpenter* protection. Applying Paul Ohm's formulation of this requirement, genetic genealogy information has the requisite depth because it is highly detailed and precise, as discussed above. And while the CSLI the Court considered in *Carpenter* was in actuality not all that accurate, the Court took into consideration the rapid development of the technology at issue and increases in accuracy certain to come.[250] Similarly, the accuracy of genetic testing technology, and the level of detail it can now reveal, has developed at a rapid clip, from the inception of CODIS in December 1990, to the first cold case suspect identified through genetic genealogy in April 2018, to more than forty

245. *Carpenter*, 138 S. Ct. at 2217 (citing United States v. Jones, 565 U.S. 400, 415 (2012)).
246. *Id.* (quoting *Jones*, 565 U.S. at 415).
247. Maryland v. King, 569 U.S. 435, 464–65 (2013).
248. Murphy, *Relative Doubt*, *supra* note 98, at 315.
249. Ram, *supra* note 141, at 12.
250. *Carpenter*, 138 S. Ct. at 2219.

by mid-2019.[251] There is no reason to suspect it will not continue to improve.

Genetic genealogy data also likely have the requisite comprehensive reach. The *Carpenter* Court noted there were, at the time the case was decided, 400 million cell phones in use in the United States, each of which essentially conveyed a log of its owner's movements to the service provider.[252] While use of genetic genealogy databases is nowhere near as pervasive, more than fifteen million people have submitted their genetic information to at least one such database, and geneticists currently predict that 60 percent of searches of DNA of Americans of Northern European descent will yield at least a third cousin, thereby making them identifiable when combined with other demographic information.[253] This percentage is expected to jump to 99 percent within a few years.[254] Thus it likely would be considered sufficiently comprehensive in nature to satisfy this requirement.

The "breadth" requirement, which refers to "how frequently the data is [sic] collected, and for how long the data has [sic] been recorded,"[255] is inapplicable to genomic data. While genetic information is only collected once per user, one's DNA is static and needs only be collected once to reveal all that it contains, unlike CSLI, which reveals more information the longer and more frequently it is recorded. Thus the "depth, breadth, and comprehensiveness" requirement is satisfied.

c. Inescapable and automatic

Genetic genealogy information fails the *Carpenter* test because its collection is not inescapable and automatic. This characteristic of CSLI data was critical to the Court's holding, as the Court was considering whether the defendant's (technically) voluntary transmission of his location information to his service provider resulting from his choice to carry a cell phone should destroy any reasonable expectation of privacy he might otherwise have had in that

251. Zhang, *supra* note 31; *Combined DNA Index System (CODIS)*, FBI, https://www.fbi.gov/services/laboratory/biometric-analysis/codis (last visited June 23, 2020).

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

253. Erlich et al., *supra* note 200, at 690.

254. *Id.*

255. Ohm, *supra* note 223, at 372.

information.[256] In holding that it should not, the Court emphasized that CSLI collection was inescapable because "cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[257] And its collection was automatic because "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up."[258]

Genomic data collection fails in both of these regards. Genetic genealogy services are not a "pervasive and insistent part of daily life." People generally use these services out of curiosity, as a hobby. There is certainly no need to do so to participate in modern society. Perhaps an argument can be made that relatives of genealogy database users had no input in the decision to upload the portions of their DNA that they share with users, and therefore the collection of their genetic data was inescapable. But this argument ignores what the Court found most compelling about the inescapable and automatic nature of CSLI collection: that it was an unavoidable byproduct of cell phone use, which was necessary to participate in modern society. "*Carpenter* applies to records that are necessarily created when a person uses core technologies of the digital age. However, it does not apply to records that a user might choose to create beyond what participation in modern Internet life requires."[259]

This requirement was also integral to the Seventh Circuit's reasoning in *Naperville Smart Meter Awareness v. City of Naperville*,[260] the only case thus far in which a federal circuit court has found *Carpenter* to apply to government collection of digital data other than CSLI.[261] There, the Seventh Circuit found the city of Naperville's installation of "smart meters" in homes, which recorded electricity consumption at fifteen minute intervals and stored the data for three years, to constitute a search under the Fourth Amendment.[262] Because different home appliances have "distinct energy-

256. *Carpenter*, 138 S. Ct. at 2217–18.
257. *Id.* at 2220 (quoting Riley v. California, 573 U.S. 373, 385 (2014)).
258. *Id.*
259. KERR, *supra* note 235 (manuscript at 3).
260. 900 F.3d 521 (7th Cir. 2018).
261. *See id.* at 527.
262. *Id.* at 524–25.

consumption patterns or 'load signatures,'"[263] the smart meter data revealed "intimate personal details of the City's electric customers such as when people are home and when the home is vacant, sleeping routines, eating routines, specific appliance types in the home and when used, and charging data for plug-in vehicles that can be used to identify travel routines and history."[264] In analyzing whether the third-party doctrine applied, the only *Carpenter* requirement the court addressed directly was whether the data collection was inescapable and automatic.[265] The Seventh Circuit determined *Carpenter* applied, and thus the third-party doctrine did not, because residents of Naperville could not choose not to have a smart meter installed in their home without forgoing electricity altogether, declaring that "a choice to share data imposed by fiat is no choice at all."[266] The court elaborated:

> If a person does not—in any meaningful sense—"voluntarily 'assume the risk' of turning over a comprehensive dossier of physical movements" by choosing to use a cell phone, it also goes that a home occupant does not assume the risk of near constant monitoring by choosing to have electricity in her home.[267]

Since this characteristic is wholly absent from genetic genealogy data, this requirement would not be satisfied. Given its importance to the Court's reasoning in *Carpenter*, this deficiency likely means genetic genealogy data obtained from consumer genomic services would not be excepted from the traditional third-party doctrine under *Carpenter*.

d. Efficiency, equilibrium-adjustment, and technological equivalence

Under a strict application of the criteria the Court articulated in *Carpenter*, genetic genealogy data accessed via consumer services would not be afforded Fourth Amendment protection. But the Court's concern with the efficiency advantage afforded law enforcement in its surveillance efforts by modern technologies—a thermal imaging

263. *Id.* at 524 (quoting Ramyar Rashed Mohassel et al., *A Survey on Advanced Metering Infrastructure*, 63 INT'L J. ELECTRICAL POWER & ENERGY SYSS. 473, 478 (2014)).

264. *Id.*

265. *Id.* at 527.

266. *Id.*

267. *Id.* (citation omitted).

camera in *Kyllo*, a GPS tracking device in *Jones*, a cell phone in *Riley*, and CSLI data in *Carpenter*—clearly applies here. Consumer genetic genealogy services represent a huge leap forward in law enforcement surveillance capabilities, granting investigators access to what in practice amounts to a genetic database of a large contingent of Americans who have committed no crimes.

Prior to a sudden advance in surveillance technology, the government's ability to surveil is constrained by practical considerations such as time, resources, and difficulty acquiring the information sought.[268] These constraints inform the types of surveillance to which society might expect to be subjected.[269] Sudden and rapid advances in surveillance technology upset these expectations.[270] As the Court noted, prior to GPS and CSLI technologies,

> law enforcement might have pursued a suspect for a brief stretch, but doing so "for any extended period of time was difficult and costly and therefore rarely undertaken." For that reason, "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement . . . for a very long period."[271]

Moreover, the Court considered societal expectations of privacy in conjunction with the "basic guideposts" of the Fourth Amendment as understood by the Founders: "First, that the Amendment seeks to secure 'the privacies of life' against 'arbitrary power.' Second, and relatedly, that a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'"[272]

Genetic genealogy investigations clearly implicate these interrelated concerns. Society's expectation of police surveillance capabilities does not include the ability to search a genetic database comprised of a large percentage of the American public. This is evident by the level of public interest in the technique and the investigations in which it has been utilized; the tenor of the conversation surrounding it; and the backlash GEDmatch received

268. United States v. Jones, 565 U.S. 400, 429 (2012) (Alito, J., concurring).
269. *Id.* at 430.
270. *See id.*
271. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (quoting *Jones*, 565 U.S. at 430).
272. *Id.* at 2214 (citations omitted).

when it contravened its own terms of service. These investigations certainly seem to utilize a "permeating police surveillance" into "the privacies of life."

The Supreme Court's attention to these concerns throughout its case law applying the Fourth Amendment to advances in surveillance technologies has informed two related but distinct theories of Fourth Amendment jurisprudence: equilibrium-adjustment and technological equivalence.

Orin Kerr's theory of equilibrium-adjustment posits that "[w]hen new tools and new practices threaten to expand or contract police power in a significant way, courts adjust the level of Fourth Amendment protection to try to restore the prior equilibrium."[273] Kerr declares *Carpenter* to be "a resounding win for the theory of equilibrium-adjustment."[274] The Court's reasoning in *Carpenter* was that

> [i]f the police can easily take investigative steps that far exceed their powers in the past . . . that newfound ability violates a reasonable expectation of privacy. . . . [T]he question is whether technological change has rendered obsolete a past expectation of a practical limit on government power.[275]

Kerr points to a crucial shift in the Court's reasoning from past precedent: "Before *Carpenter*, the *Katz* test was about places and things. The law asked whether government action violated a reasonable expectation of privacy in a particular place or thing. *Carpenter* asks a different question: Has technology changed expectations of *what the police can do*?"[276] He acknowledges the importance of the information's deeply revealing nature but argues that

> [t]he trigger for the search was not the details of what the police learned about Carpenter in that particular case. Instead, the trigger was the broader technological shift that enabled the police to learn a lot about everyone who used a

273. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480 (2011).

274. KERR, *supra* note 235 (manuscript at 1).

275. *Id.* (manuscript at 8).

276. *Id.* (manuscript at 7) (emphasis in original).

> cell phone—that is, everyone. It's as if the technology violated a reasonable expectation of privacy rather than the government.[277]

The theory of technological equivalence similarly focuses on the rapid development of surveillance technology and the effect it has on society's expectation of privacy as a whole.

> At least seven justices of the *Carpenter* Court suggest a heretofore unrecognized rule building on *Kyllo*: the *rule of technological equivalence*. If a technology, or near-future improvement, gives police the power to gather information that is the "modern-day equivalent" of activity that has been held to be a Fourth Amendment search, the use of that technology is also a search.[278]

Paul Ohm argues that previously, "the Supreme Court has tended to pay more attention to the nature of the police intrusion required to obtain information than to the nature of the information obtained."[279] In *Carpenter*, however, the Court focused on whether there is a reasonable expectation of privacy in the data themselves, viewed in isolation.[280] Critical to this analysis was whether this was information previously accessible to law enforcement, either at all or without a prohibitively expensive allocation of resources, prior to the advent of the technology utilized to access the data.[281] Ohm ties technological equivalence to equilibrium-adjustment in arguing that the objective prong of the "reasonable expectation of privacy" test should be purely normative, rather than descriptive: courts should consider whether the type and extent of surveillance made possible by a new technology are acceptable to society, or whether they instead should be limited or proscribed, without attempting to discern how society might actually feel about the technology at that moment in time.[282]

Commercial genetic genealogy investigations and the data they reveal fail a mechanical application of *Carpenter* because the data collection is not inescapable or automatic, critical to the Court's

277. *Id.* (manuscript at 10).
278. Ohm, *supra* note 223, at 359–60 (emphasis in original).
279. *Id.* at 362.
280. *Id.* at 362–63.
281. *See id.* at 367–68
282. *Id.* at 387–88.

analysis in *Carpenter* and the extension of its holding to any new type of database.[283] Not only do users provide the information to the databases voluntarily, they do so for the express purpose of making connections to other users and investigating one's family tree. But genetic genealogy investigations by law enforcement trigger the same broad concerns that inform equilibrium-adjustment and technological equivalence. Indeed, this new investigative technique intuitively seems like it should qualify for protection under *Carpenter*, for it has raised serious privacy concerns amongst the public and sparked user backlash against consumer genomic service providers that have relaxed or violated their privacy policies by cooperating with law enforcement.

Commercial genealogy databases greatly increase police power to investigate crimes—not only decades' old cold cases, but recently committed crimes in real time—by utilizing what is rapidly becoming the functional equivalent of a genetic database of a large portion of Americans. Law enforcement in Centerville, Utah used the technique to catch an assailant who was still at large only a few months after he assaulted a woman at a local church.[284] Investigations that took weeks in early 2018 are now identifying suspects in a matter of days.[285] Police power has clearly expanded in a very significant way. Under the theory of equilibrium-adjustment, courts should be expected to respond in kind to restore balance. It is reasonable to assume that society's current expectation is that police do not have access to a database of the DNA of millions of people, who have committed no crime, that police cannot utilize such database to identify them or their relatives in the course of investigating a crime, while simultaneously accessing a wealth of intimate biological information derived from their genomes.

And the theory of technological equivalence should similarly advocate for Fourth Amendment protection of commercial genomic databases. Comparing a genetic sample retrieved at a crime scene to a database of millions of Americans would have been inconceivable to

283. *See id*. at 376–77; Freiwald & Smith, *supra* note 229, at 219–20; KERR, *supra* note 235 (manuscript at 3).

284. Aldhous, *supra* note 80.

285. Megan Molteni, *The Key to Cracking Cold Cases Might Be Genealogy Sites*, WIRED (June 1, 2018, 7:00 AM), https://www.wired.com/story/police-will-crack-a-lot-more-cold-cases-with-dna/.

the Founders. And as recently as 2013, the Supreme Court in *King* emphasized that "[i]f 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."[286] The dissent warned that law enforcement would be able to collect DNA from individuals for even minor offenses and thereby build a national database.[287] Indeed, private companies have created what will soon be the functional equivalent of a national genetic database at law enforcement's disposal. Because genetic genealogy investigations utilize a new technology to acquire information that just six years ago the Supreme Court acknowledged, at least implicitly, would constitute a search, the theory of technological equivalence says such investigations should be treated as searches under the Fourth Amendment.

While both equilibrium-adjustment and technological equivalence seem to argue in favor of treating genetic genealogy investigations as Fourth Amendment searches, the technique simply does not fit the *Carpenter* test, and thus, absent further extension of *Carpenter* by courts, would not constitute a search.

C. Assuming a Search—Is It Lawful?

Were courts to extend *Carpenter* such that forensic genetic genealogy would constitute a search under the Fourth Amendment, the technique would be lawful only if conducted pursuant to a warrant, or if deemed reasonable by courts. Because obtaining a warrant would be impracticable, if not impossible, courts would employ a balancing test, weighing law enforcement interests against privacy interests,[288] likely finding such searches reasonable when employed to solve particularly heinous crimes, but not lesser ones.

1. The Warrant Preference

First, while obtaining a warrant would make such a search presumptively reasonable,[289] courts would likely deem warrants to be impracticable and therefore not required, notwithstanding that a judge

286. Maryland v. King, 569 U.S. 435, 464–65 (2013).
287. *Id.* at 481 (Scalia, J., dissenting).
288. *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 20–21 (1968).
289. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

recently issued such a warrant for the first time. In July 2019, Judge Patricia Strowbridge of the Ninth Judicial Circuit Court of Florida issued a warrant to a Florida detective to override GEDmatch's recently enacted automatic opt-out privacy policy, thus allowing him to search the entire database.[290] Whether this constitutes an outlier or the first of many remains to be seen. The actual warrant and application have not been released publicly, but it is likely Judge Strowbridge did not consider law enforcement's use of GEDmatch to be a search of records in which the users had a reasonable expectation of privacy. Rather, she likely considered the GEDmatch database and the genetic information contained therein to be GEDmatch's proprietary records, under the third-party doctrine, so the warrant was likely written to override any objection GEDmatch might have made to the search, without addressing the users at all. Probable cause was likely supported solely by the success rate of such investigations in identifying a suspect, currently 60 percent if the perpetrator is Caucasian and of Northern European descent.[291] This is concerning in and of itself, for if law enforcement's justification for accessing these records is based on the third-party doctrine, an explicit opt-out should counter that rationale.[292] But if courts extend *Carpenter* to find that GEDmatch users and their relatives have a reasonable expectation of privacy in their genetic data, this line of reasoning would not hold up, and obtaining a warrant would be impracticable, if not impossible. There would be no way to describe the exact persons to be searched, other than to search each of the millions of databased individuals, much like the general warrants the Fourth Amendment was designed to protect against.[293]

290. Hill & Murphy, *supra* note 12.

291. Erlich et al., *supra* note 200.

292. *See* Aaron Mak, *We May Be Entering a New Era for Using Consumer Genetic Information to Solve Crimes*, SLATE (Nov. 8, 2019, 4:01 PM), https://slate.com/technology/2019/11/gedmatch-warrant-dna-ancestry-23andme.html ("'Law enforcement has repeatedly asserted that the reason it's OK for them to use this kind of consumer genetics data is because it's all voluntarily shared,' says Natalie Ram, an associate law professor at the University of Maryland. 'To then override an explicit opt-out seems quite troubling.'").

293. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2213 ("The Founding generation crafted the Fourth Amendment as a 'response to the reviled "general warrants" and "writs of assistance" of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.'" (quoting Riley v. California, 573 U.S. 373, 403 (2014))).

2. Individualized Suspicion

Absent a warrant, courts must deem genetic genealogy investigations reasonable to be lawful. But the lack of individualized suspicion inherent in such searches poses a major impediment to validating them based on a traditional reasonableness balancing inquiry. For a search to be reasonable, the Fourth Amendment requires some level of individualized suspicion—either probable cause or reasonable suspicion—to support law enforcement's belief that searching the individual will lead to evidence of the crime being investigated.[294] Here, there would be none, as it would be impossible for law enforcement to have any specific, articulable facts informing a belief that the search of the profile of a specific person in the database will yield a connection to an unknown perpetrator's genetic material. And, because these searches are for normal criminal investigative purposes, they cannot readily be justified as special needs searches, which do not require individualized suspicion.[295]

CODIS searches lack individualized suspicion in much the same way as forensic genealogy searches, but are nonetheless considered constitutional under *King*.[296] But the Supreme Court in *King* considered the search at issue to be the acquisition of genetic samples from arrestees, not the practice of uploading those samples to CODIS and looking for matching profiles.[297] The Court accepted that the primary purpose of DNA collection and storage was to more accurately identify arrestees, rather than to generate leads in unsolved crimes. Because the search was of an individual arrestee with a diminished expectation of privacy, there was no individualized suspicion issue, so the Court conducted a balancing test and found the search reasonable.[298]

The dissent, however, correctly identified the primary state interest in maintaining CODIS—matching unidentified genetic evidence to databased individuals to identify suspects.[299] Accordingly, the dissent excoriated the majority for even conducting a balancing

294. *See, e.g.*, City of Indianapolis v. Edmond, 531 U.S. 32, 37 (2000) ("A search or seizure is ordinarily unreasonable in the absence of individualized suspicion of wrongdoing.").

295. *See id.* at 41–42.

296. *See* Maryland v. King, 569 U.S. 435, 452 (2013).

297. *Id.* at 446.

298. *Id.* at 464.

299. *Id.* at 469 (Scalia, J., dissenting).

test in the first place, because "[n]o matter the degree of invasiveness, suspicionless searches are *never* allowed if their principal end is ordinary crime-solving."[300] Here, forensic genetic genealogy investigations by law enforcement serve no plausible alternative purpose other than criminal investigation that might allow a court to get around a lack of individualized suspicion to even conduct a reasonableness balancing test, and thus such searches should be unlawful.

3. Reasonableness

Were a court to put aside the lack of individualized suspicion, such searches would likely be found reasonable only when the crimes at issue are particularly severe. The state interests in utilizing this technique are compelling. There is a strong state interest in solving crime, of course, and in particular especially violent crimes that have proven unsolvable by traditional means. Moreover, the technique will likely prove valuable in exonerating wrongfully convicted individuals by buttressing evidence of mismatched DNA with compelling evidence that someone else entirely was the actual perpetrator. Further, solving decades-old cold cases can bring closure and emotional relief to families that have suffered for years. And the technique has already proven effective, reliable and efficient at doing so. However, the state interests weaken as the crimes become less severe and the need to solve them becomes less critical. They may further weaken when traditional investigative techniques have not yet been exhausted, and thus may still prove successful.

The privacy interests implicated are compelling as well, and genealogical investigations can be quite intrusive. One's genetic information is intimate, detailed, and highly revealing. It can reveal unknown or undisclosed personal traits, predisposition to diseases and other ailments, and other private information. It can also reveal private or unknown family relationships, which could prove devastating if disclosed. Such information is certainly as revealing and thus as intrusive as CSLI.[301] Further, the technique casts suspicion on many

300. *Id.* (emphasis in original).

301. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217–18 (2018) ("[T]he time-stamped data provides [sic] an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual

people for no reason other than an immutable genetic connection. Such suspicion, and traditional forms of investigation that might follow, can greatly affect one's reputation, career, and personal relationships.

Thus, balancing these competing interests, a court would likely find forensic genetic genealogy investigations reasonable when the state interests are strongest: when the crime at issue is particularly severe, such as homicide and certain violent or sexual crimes, and when all other investigative techniques have been exhausted. Under these circumstances, the state interests are significantly stronger than they were in *Carpenter*, and thus the balance would tip in favor of the government. However, absent these circumstances, if forensic genealogy were being used to investigate more common crimes right after they occur, where traditional investigative techniques were still available, then the reasonableness balancing analysis should track *Carpenter*, and courts should find these searches to be unreasonable.

V. POLICY AND LEGISLATIVE CONSIDERATIONS

Law enforcement's use of forensic genetic genealogy to investigate crimes is not currently governed by any legislation or regulations, and is proliferating rapidly.[302] Given the sensitivity and intimate nature of genetic information, how intrusive forensic genetic genealogy investigations can be, and that the Fourth Amendment likely provides no constraints under current jurisprudence, it is critical that legislation be crafted to provide guidance and set boundaries. Public sentiment regarding the practice is conflicted and unclear, and database privacy policies alone are insufficient to provide adequate protection of people's private genetic information, especially if warrants overriding such protections become more common. Maryland has already introduced a bill banning the technique outright, but it has not yet been enacted.[303] Given the compelling state interests the technique serves, the privacy concerns it implicates, and the conflicted state of public sentiment regarding both, legislators and the public at large must weigh a number of factors in order to properly

associations.' These location records 'hold for many Americans the "privacies of life."'" (quoting first United States v. Jones, 565 U.S. 400, 945 (2012) and then Riley v. California, 573 U.S. 373, 403 (2014))).

302. Zhang, *supra* note 31.

303. *See* H.B. 30, 439th Gen. Assemb., Reg. Sess. (Md. 2019).

balance state and private interests and delineate acceptable parameters for this method of criminal investigation.

Public sentiment regarding the technique is difficult to accurately gauge. Two separate 2018 studies suggest the public supports law enforcement's use of their genetic data to solve particularly serious crimes. The first, a self-published survey genealogist Maurice Gleeson conducted of other genealogists, found that 85 percent of respondents were "reasonably comfortable" when their DNA was being used to solve homicides and serial rapes, but only 47 percent were supportive when used to solve lesser crimes.[304] A more formal study published in October 2018 by a group of researchers led by Christina J. Guerrini at the Center for Medical Ethics and Health Policy at Baylor College of Medicine in Houston, Texas, contained similar findings:

> Among the 1,587 respondents, the majority supported police searches of genetic websites that identify genetic relatives (79%) and disclosure of [direct-to-consumer] genetic testing customer information to police (62%), as well as the creation of fake profiles of individuals by police on genealogy websites (65%). However, respondents were significantly more supportive of these activities (all $p < 0.05$) when the purpose is to identify perpetrators of violent crimes (80%), perpetrators of crimes against children (78%), or missing persons (77%) than when the purpose is to identify perpetrators of nonviolent crimes (39%).[305]

The authors note they found the same pattern and rates of approval for law enforcement use of CSLI.[306]

Yet the notion that the public overwhelmingly approves of law enforcement's use of everyone's DNA to solve violent crimes is belied by certain anecdotal evidence to the contrary. When FamilyTreeDNA disclosed that it had agreed to grant the FBI access to its database on a case by case basis, many of its users were outraged.[307] "All in all, I

304. Tashea, *supra* note 90.

305. Christina J. Guerrini et al., *Should Police Have Access to Genetic Genealogy Databases? Capturing the Golden State Killer and Other Criminals Using a Controversial New Forensic Technique*, PLOS BIOLOGY (Oct. 2, 2018), https://doi.org/10.1371/journal.pbio.2006906.

306. *Id.*

307. Salvador Hernandez, *One of The Biggest At-Home DNA Testing Companies Is Working with the FBI*, BUZZFEED NEWS (Jan. 31, 2019, 8:52 PM),

feel violated, I feel they have violated my trust as a customer," one user told *Buzzfeed News*, who first uncovered the cooperation agreement, forcing the disclosure.[308] Most other prominent consumer genetic service providers do not cooperate with law enforcement, deny requests for information, and resist subpoenas.[309] 23andMe released the following statement when asked about the implications of the Florida warrant: "We never share customer data with law enforcement unless we receive a legally valid request such as a search warrant or written court order. Upon receipt of an inquiry from law enforcement, we use all practical legal measures to challenge such requests in order to protect our customers' privacy."[310] Such practices reflect a general understanding amongst these companies that their customers would be uncomfortable with routine use of their DNA in criminal investigations, for it would certainly be easier and cheaper for these companies to cooperate. And law enforcement practice reflects a similar recognition of public unease. The law enforcement community has admitted to being reluctant to use court orders to gain access to commercial genealogy databases for fear of scaring users away.[311]

Public sentiment may turn not only on the severity of the crime but on whether these investigations feel like contemporaneous and pervasive surveillance. This, in turn, may be informed by whether the crime being investigated was recently committed, or is old and cold. User backlash, when GEDmatch violated its own terms of service to allow law enforcement to access its database to solve the assault of a woman in Utah, led it to institute its automatic opt-out policy.[312] That the crime at issue was less severe than what GEDmatch's previous terms of service allowed for—homicide or sexual assault—certainly contributed to the user backlash.[313] But the crime was nevertheless severe: the perpetrator attacked a seventy-one-year-old woman in a church and choked her until she lost consciousness.[314] User backlash

https://www.buzzfeednews.com/article/salvadorhernandez/family-tree-dna-fbi-investigative-genealogy-privacy.

308. *Id.*

309. Hill & Murphy, *supra* note 12.

310. *Id.*

311. *Id.*

312. Aldhous, *supra* note 74.

313. *See GEDMatch.Com Terms of Service and Privacy Policy*, *supra* note 75 (version prior to May 18, 2019 update).

314. Reavy, *supra* note 77.

was likely also due to the real-time nature of the investigation. This was not a decades-old cold case—the crime had been committed only a few months prior to GEDmatch granting access, and the perpetrator was still at large.[315] Thus, the backlash was most likely the product not only of the lessened severity of the crime, but also the sense of pervasive surveillance that investigations such as this one take on, where the crimes are fresh, the cases are active, and other investigatory techniques have not yet been exhausted.

Last, people may feel comfortable with the idea of law enforcement using their DNA to investigate crimes in the abstract, but less so in practice, and so might respond positively to a survey but feel violated when their own data are actually accessed and utilized. Indeed, since October 1, 2019, only 185,000 GEDmatch users have opted-in to allow law enforcement matching,[316] indicating a lack of enthusiasm, at best, for participating personally in these investigations.

Given the unsettled and conflicted nature of public sentiment, and past instances of commercial genetic genealogy companies failing to properly anticipate their users' reactions to decisions to either violate their own terms of service or unilaterally change them, it is clear users cannot rely on company privacy policies to provide sufficient protection. While certain databases' terms of service have thus far provided robust protection, such as those of Ancestry and 23andMe, which do not voluntarily cooperate with law enforcement and fight court orders and subpoenas, others are far laxer. And even if a database enforces a robust privacy policy, courts may decide to follow the lead of Florida's Ninth Judicial Circuit Court and issue warrants granting law enforcement access. While GEDmatch did not challenge the validity of the warrant, 23andMe has stated it would fight any warrants it receives, and so a proliferation of warrants does not seem imminent just yet. But even so, given the already unreliable nature of privacy policies, and the possibility of more warrants, such policies do not provide sufficient protection for database users' and their relatives' genetic data. Legislation is therefore needed.

Maryland is currently the only state to have proposed a bill that would restrict law enforcement's use of forensic genetic genealogy.

315. *Id.*
316. Hill & Murphy, *supra* note 12.

Maryland House Delegate Charles Sydnor III introduced House Bill 30 at the first legislative session of 2019, which would have prohibited law enforcement from utilizing commercial genetic databases in criminal investigations entirely.[317] The bill did not make it out of committee, but Mr. Sydnor plans to introduce a revised version in 2020.[318] "The policy in the state of Maryland is pretty clear: We shouldn't be doing this," he has stated.[319] Maryland is also one of only two states with statutes prohibiting FDS.[320]

It seems unlikely, however, that a complete ban comports with public sentiment either. Given the compelling need to solve particularly heinous crimes, especially those that have been cold for decades, a complete ban would be misguided. Rather, legislation should be carefully crafted that seeks to properly balance the needs of law enforcement to solve these crimes, with the privacy interests of what will soon be the large majority of the American populace identifiable through one of these databases. Legislation should, at least initially, be drawn narrowly, so law enforcement can only access the public's sensitive genetic information in the most compelling of circumstances. With time, as law enforcement becomes better skilled at the technique, privacy safeguards are implemented and proven effective, and the public becomes accustomed to widespread use of the technique, use restrictions can be reevaluated, and perhaps loosened. Any legislation will need to address the following considerations.

A. Type of Crime

Effective legislation governing law enforcement's use of forensic genetic genealogy to solve crimes must clearly define the crimes for which law enforcement will be permitted to use the technique. Public sentiment seems to draw the line at homicide and violent crimes. This is reflected in both 2018 studies discussed above, as well as anecdotal evidence. In both the study by Maurice Gleeson and the study by Christina J. Guerrini, respondents overwhelmingly approved of law enforcement's use of their DNA to solve violent crimes, but support

317. H.B. 30, 439th Gen. Assemb., Reg. Sess. (Md. 2019).
318. Tashea, *supra* note 90.
319. *Id.*
320. Ram, *supra* note 141, at 11.

dropped by roughly half for nonviolent crimes.[321] Moreover, before GEDmatch instituted its automatic opt-out policy, its terms of service made clear it allowed law enforcement use of the database to solve "violent crime," which it defined as "homicide or sexual assault."[322] GEDmatch's 1.2 million users chose to entrust their genetic data to the company under these conditions. But when GEDmatch allowed law enforcement to search the database to investigate an aggravated assault, user backlash ensued.

This calculation also reflects the inflection point where courts would likely find the use of this technique, if deemed a Fourth Amendment search, to be reasonable. Solving violent crimes is a stronger state interest than solving nonviolent ones, and thus likely outweighs the public's privacy interests in its genetic information. For nonviolent crimes, courts following *Carpenter* should find the balance to track that which the Court at least implicitly struck between the state's interest in investigating serial robberies and the public's reasonable expectation of privacy in its CSLI data, and should therefore find the use of forensic genealogy unreasonable in these cases.

Accordingly, the line should, at least initially, be drawn at violent crimes, as defined by GEDmatch's prior terms of service—homicides and sexual assaults. Because initial legislation should be as narrow as possible, erring on the side of protecting privacy, and can be expanded later as public sentiment shifts, the technique should also be limited to investigating those sexual assaults in which the perpetrator is implicated in multiple such crimes, rather than single crimes. While this might prove controversial, such a requirement can always be revised downward later, if supported by the public at large.

B. Time Elapsed Since Crime

Legislation should also limit use of forensic genetic genealogy to investigate crimes that have gone cold for some defined amount of time. Where to draw that line is a difficult question that will surely be the subject of much debate, but society seems to be more comfortable with law enforcement using commercial DNA databases to solve the decades-old Golden State Killer case than to solve the months-old

321. Guerrini et al., *supra* note 305; Tashea, *supra* note 90.

322. *GEDMatch.Com Terms of Service and Privacy Policy*, *supra* note 75 (version prior to May 18, 2019 update).

Washington aggravated assault. While the backlash against GEDmatch in the Washington case was due in part to the crime being less severe than the terms of service required, the contemporaneous nature of law enforcement's use of the service to identify a perpetrator on the loose for a crime very recently committed has the feel of a more pervasive surveillance that likely caused many people discomfort.

This will undoubtedly prove controversial as well. The need to catch perpetrators who have recently committed violent crimes and are still at large, and prevent them from striking again, is arguably greater than the need to identify now-geriatric killers and rapists whose cases have long since gone cold and most likely no longer pose an active threat to society. But requiring a certain period of time to have lapsed before law enforcement may utilize private DNA data prevents the users from having the feel of contemporaneous surveillance. It would also cause the purpose of the investigation to less closely resemble regular run-of-the-mill crime fighting and instead resemble a special needs search. The purpose of the search could be framed not as ordinary criminal investigation to catch an offender currently posing a danger to the public, but as bringing closure to victims' families by finally resolving long unsolved cases. While courts are more comfortable with law enforcement searches absent individualized suspicion if serving a special need other than ordinary criminal investigation,[323] it remains to be seen if such a distinction will matter to the public, and therefore to legislators.

C. Exhaustion of Other Investigatory Techniques

Legislation should also require law enforcement to have exhausted all traditional, reasonable investigative techniques before turning to genetic genealogy. This would work in conjunction with a minimum elapsed time requirement, affording law enforcement the time needed to exhaust other techniques. This would ensure law enforcement would only access people's private, sensitive genetic data in the most compelling of circumstances.

D. Training and Safeguards

Legislation should impose training and procedural requirements on law enforcement to ensure genetic genealogical investigations are

323. *See* City of Indianapolis v. Edmond, 531 U.S. 32, 41–42 (2000).

narrow in scope and ethically conducted. Effective legislation must also adequately safeguard sensitive genetic data and the intimate, personal information that can be uncovered by digging into a person's family tree. Protective procedures should be implemented to ensure private personal information, such as genetic predispositions for certain diseases, or unknown or undisclosed familial relationships, is not accidentally revealed during the course of an investigation, either to a subject of investigation or publicly. Such accidental disclosures can destroy reputations, careers, friendships and families, and must be effectively prevented.

Moreover, training should focus on narrowing the scope of genealogical investigations by teaching law enforcement agencies how to properly conduct the most efficient investigation possible. This would minimize the number of individuals upon whom suspicion is cast, so as few people as possible are subjected to intrusive investigation. Genealogist CeCe Moore has expressed support for an industry certification requirement for genealogists conducting criminal investigations, but support amongst her colleagues is weak.[324] Effective legislation must impose such a requirement.

E. Evolution of Technology

Last, effective legislation must consider the rapid evolution of forensic genetic genealogy technology and be adaptable accordingly. Limits on the technique should start quite narrowly, erring on the side of privacy protection. These limits may be relaxed over time, if training and procedural safeguards prove effective and public sentiment supports broadening the technique's application. But as the technology continues to become more efficient and cheaper, the temptation to deploy it for lesser crimes will grow. As more people continue to entrust their genetic data to these commercial databases, and as algorithms improve to allow connections to fourth and fifth cousins, instead of just third, the functional equivalent of a national genetic database will emerge. Such developments would militate against a loosening of the restrictions endorsed above. Ultimately, legislators and the public will have to monitor the development of this technology in order to ensure an acceptable balance between privacy and law enforcement interests is maintained.

---

324. Tashea, *supra* note 90.

VI. CONCLUSION

The use of commercial genetic genealogy in criminal investigations is expanding rapidly, and the technique is quickly becoming faster and more efficient. The existence of the functional equivalent of a national genetic database is imminent, raising serious privacy concerns, but also creating important tools for law enforcement. Commercial genealogy service providers have attempted to implement privacy policies that strike the proper balance between governmental and personal privacy interests, but they have proven inconsistent and unreliable. And the Fourth Amendment likely does not apply, even under *Carpenter*. This is so even though the technique greatly enhances law enforcement surveillance power in a manner that should trigger an expansion of the Fourth Amendment under the theories of equilibrium-adjustment and technological equivalence. Absent such an expansion, it is critical legislation be enacted to protect the wealth of intimate personal information that genetic genealogy can reveal and prevent abuse by law enforcement. Such legislation should initially be drawn narrowly, permitting law enforcement to utilize the technique only to solve the most serious crimes, after a prescribed period of time, and when all other methods of investigation have been exhausted. Law enforcement should have access to this incredibly potent tool, but only when absolutely necessary. Thorough training and strict procedural protections must be implemented, for genetic genealogical investigations should only be permitted if the public's privacy interest in its own intimate genetic, biological, and personal information can be ensured.