GENETIC PRIVACY: LATE TO THE THIRD PARTY

CIERA GONZALEZ*

Beginning with the capture of the Golden State Killer in April of 2018, law enforcement has increasingly turned to public genealogy databases such as GEDmatch to identify suspects in unsolved crimes. Websites like GEDmatch are typically used by individuals seeking information about their ancestry, but law enforcement has found that by uploading DNA profiles of unknown crime suspects to these websites they can look for partial or complete matches between their suspect and those who have uploaded their own DNA. As more individuals upload their genetic information to these sites and law enforcement searches of these genealogical databases increase, the debate surrounding the Fourth Amendment, the third-party doctrine, and the rightful balance between individual privacy and law enforcement's ability to ensure community safety is heating up.

The Fourth Amendment protects people from unlawful searches and seizures, but the third-party doctrine creates an exception. The third-party doctrine holds that people who voluntarily give information to third parties have no reasonable expectation of privacy in that information. As the third-party doctrine is traditionally understood, individuals who have uploaded their genetic information to public databases like GEDmatch have no expectation of privacy in that information. Thus, law enforcement's warrantless search of the genetic information stored in the database does not violate the Fourth Amendment. But a recent U.S. Supreme Court Case, Carpenter v. United States*, has shed new light on the third-party doctrine. This Note considers the privacy implications of law enforcement searches of public genealogy databases, whether the ruling in* Carpenter *could be read to protect user-submitted genetic information under the Fourth Amendment, and how best to protect genetic privacy going forward.*

* J.D., University of Colorado, Class of 2020; B.A., University of Tampa, Class of 2016.

INTRODUCTION

For four decades, law enforcement tried and failed to identify the individual responsible for dozens of murders and rapes throughout California in the 1970s and 1980s.[1] Traditional investigative techniques came up empty. But an innovative new method employed by an investigator in 2018 finally led to the arrest of the infamous criminal known as the Golden State Killer.[2] The arrest of

1. *See* Thomas Fuller & Christine Hauser, *Search for 'Golden State Killer' Leads to Arrest of Ex-Cop*, N.Y. TIMES (Apr. 25, 2018), https://www.nytimes.com/2018/04/25/us/golden-state-killer-serial.html [https://perma.cc/3NYT-RJFS].

2. Justin Jouvenal, *To Find Alleged Golden State Killer, Investigators First Found His Great-Great-Great Grandparents*, WASH. POST (Apr. 30, 2018, 4:22 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-

Joseph DeAngelo was a win for law enforcement and the community at large, but when the method used to identify DeAngelo as the Golden State Killer was revealed, privacy experts were alarmed.[3] Without a suspect in mind, investigators took the deoxyribonucleic acid ("DNA") recovered from one of the Golden State Killer's crime scenes and uploaded it to GEDmatch, a public genealogy website filled with the profiles of individuals who volunteered their genetic information to discover their ancestry.[4] Investigators did not find the perfect match in the database because DeAngelo's DNA was not in the site's database.[5] However, the DNA of one of his family members was in the database, and the crime scene DNA partially matched with one of the killer's distant relatives.[6] Starting with that distant family member, detectives built out the family tree until they found a family member who matched what officers were looking for in a suspect: Joseph DeAngelo.[7] Investigators then collected an item discarded by DeAngelo and tested his DNA against the killer's.[8] It was a match, and Joseph DeAngelo was arrested on April 24, 2019.[9] Following the success of the Golden State Killer investigation, investigators across the country adopted the genealogical search technique to arrest more than twenty people tied to cold cases.[10] The technique is well "on its way to becoming a routine police procedure."[11]

4a0e-b6b2-0bec548d501f [https://perma.cc/HE3G-PB36] (discussing how investigator Paul Holes used genetic mapping to catch the killer, where DNA, fingerprints and offering hefty rewards could not).

3. *See, e.g.*, Adhiti Bandlamudi, *Tactics Used to Find Golden State Killer Raise Privacy and Legal Questions*, NAT'L PUB. RADIO (Apr. 27, 2018, 4:22 PM), https://www.npr.org/2018/04/27/606580162/tactics-used-to-find-golden-state-killer-raise-privacy-and-legal-questions [https://perma.cc/Y78J-FT48]; Connecticut Editorial Board, *Golden State Killer Case Raises Legal, Ethical DNA Issues*, CONN. L. TRIB. (June 8, 2018, 3:59 PM), https://www.law.com/ctlawtribune/2018/06/08/golden-state-killer-case-raises-legal-ethical-dna-issues [https://perma.cc/D422-UYE3].

4. Avi Selk, *The Ingenious and 'Dystopian' DNA Technique Police Used to Hunt the 'Golden State Killer' Suspect*, WASH. POST (Apr. 28, 2018, 7:50 AM), https://www.sltrib.com/news/nation-world/2018/04/28/the-ingenious-and-dystopian-dna-technique-police-used-to-hunt-the-golden-state-killer-suspect/ [https://perma.cc/6GGF-EVYA].

5. *Id.*

6. *Id.*

7. *Id.*

8. Jouvenal, *supra* note 2, at 3.

9. *Id.*

10. *See* Sarah Zhang, *How a Tiny Website Became the Police's Go-To Genealogy Database*, THE ATLANTIC (June 1, 2018), https://www.theatlantic.com/science/archive/2018/06/gedmatch-police-genealogy-database/561695 [https://perma.cc/SJ5T-4YVA]; Megan Molteni, *The Future of Crime-Fighting is Family Tree Genetics,* WIRED (Dec. 26, 2018, 8:00 AM), https://www.wired.com/story/the-future-of-crime-fighting-is-family-tree-forensics [https://perma.cc/DX99-5VQ4].

11. Molteni, *supra* note 10.

Privacy experts are not so sure this is a good thing.[12] Currently, the warrantless searches of these databases conducted by law enforcement do not appear to violate the Fourth Amendment. This is because DNA in genealogical databases like GEDmatch falls under the Fourth Amendment's third-party doctrine, which says that people who voluntarily give information to third parties no longer have a reasonable expectation of privacy over that information.[13] Thus, because it was actually DeAngelo's distant relative whose DNA was searched, and they uploaded their DNA to the site voluntarily, this search method does not necessarily raise a Fourth Amendment problem. Yet, few realize that when they go searching for long lost family members on genealogical sites, they are exposing both themselves and their relatives to potential searches by law enforcement.[14] The third-party doctrine—already a source of frustration for many legal scholars[15]—is ill-equipped to handle the many technological advances that lead us to reveal a vast amount of information to third parties today.

In 2018, the Supreme Court took a fresh look at the third-party doctrine in *Carpenter v. United States,*[16] which considered whether law enforcement could access cell-site location information ("CSLI")[17] without a warrant.[18] In a narrow decision, the majority declined to extend (but did not overrule) existing third-party

12. *See* Bandlamudi, *supra* note 3, at 3; *see also Golden State Killer Arrest is Cause for Celebration — and Some Concern over DNA Privacy*, PBS NEWS HOUR (May 1, 2018, 6:25 PM), https://www.pbs.org/newshour/show/golden-state-killer-arrest-is-cause-for-celebration-and-some-concern-over-dna-privacy [https://perma.cc/G4GY-HPYQ].

13. *See* United States v. Miller, 425 U.S. 435, 443 (1976) ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."); *see also* Max Mitchell, *As Genealogy Databases Aid in Crime-Solving, Are Courts Ready to Tackle DNA Privacy?*, LAW.COM (July 23, 2018, 1:56 PM), https://www.law.com/thelegalintelligencer/2018/07/23/as-genealogy-databases-aid-in-crime-solving-are-courts-ready-to-tackle-dna-privacy [ttps://perma.cc/9UWL-6W42].

14. *See* discussion *infra* Sections I.B, I.C.

15. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563-64 (2009).

16. Carpenter v. United States, 138 S. Ct. 2206, 2209 (2018).

17. *Id.* at 2211–12 (Chief Justice Roberts explained the way this technology works: "Cell phones perform their wide and growing variety of functions by connecting to a set of radio antennas called 'cell sites' . . . Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI). The precision of this information depends on the size of the geographic area covered by the cell site. The greater the concentration of cell sites, the smaller the coverage area. As data usage from cell phones has increased, wireless carriers have installed more cell sites to handle the traffic. That has led to increasingly compact coverage areas, especially in urban areas . . . While carriers have long retained CSLI for the start and end of incoming calls, in recent years phone companies have also collected location information from the transmission of text messages and routine data connections. Accordingly, modern cell phones generate increasingly vast amounts of increasingly precise CSLI.").

18. *Id.* at 2206.

doctrine precedent to the cell-site information at issue in that case.[19] The majority reasoned the cell records were unique in nature and declared "the fact that information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[20] The Court concluded that in this case the search violated Carpenter's reasonable expectation of privacy, but made no broader claims about the third-party doctrine's future applicability.[21] In his dissent, Justice Gorsuch recognized the dangers of the *Carpenter* Court's decision not to directly overrule existing precedent.[22] Justice Gorsuch imagined a case involving a search of DNA from genealogical databases and noted that as the third-party doctrine is interpreted today, law enforcement would have no trouble securing that DNA without a warrant or probable cause.[23]

The third-party doctrine is based on the idea that one assumes the risk that their information will end up in the hands of police by giving that information up to a third party.[24] But under *Carpenter*, it appears that the nature and use of the information should also be a factor when evaluating whether an individual assumed that risk.[25] As law enforcement increases its use of public genealogical databases, clarity is needed regarding how the third-party doctrine should apply to voluntarily submitted genetic information. If the *Carpenter* majority's rationale is applied to a case involving genetic information, a court could find that because of the nature of genetic information, an individual maintains their expectation of privacy from law enforcement access despite having voluntarily submitted to a third-party genealogy database.

This Note considers the privacy implications of law enforcement searches of public genealogy databases and whether the ruling in *Carpenter* could be read to protect user-submitted genetic information from warrantless searches under the Fourth Amendment. Part I of this Note explains the DNA databases traditionally used by law enforcement for investigations and contrasts that use with law enforcement use of public genealogy databases like GEDmatch. Part II addresses the development of the third-party doctrine and where it stands today. Part III analyzes how courts might interpret the *Carpenter* decision to protect a person's privacy rights of their DNA in a genealogical database like

19. *Id.* at 2216–17.
20. *Id.*
21. *Id.*
22. *Id.* at 2262 (Gorsuch, J., dissenting).
23. *Id.* ("Can [the government] secure your DNA from 23andMe without a warrant or probable cause? *Smith* and *Miller* say yes it can—at least without running afoul of *Katz*. But that result strikes most lawyers and judges today—me included—as pretty unlikely.").
24. Kerr, *supra* note 15, at 563.
25. *See* Carpenter v. United States, 138 S. Ct. 2206, 221–718 (2018).

GEDmatch. Part IV suggests solutions to the problematic privacy implications of law enforcement searches of DNA databases: I propose a new third-party doctrine framework supported by *Carpenter*, and legislative solutions to protect individual privacy in sensitive genetic information.

I. THE MAKING OF A DNA DATABASE

Investigative searches of DNA databases by law enforcement are not a new phenomenon. The first reported use of DNA evidence by an American court came in 1988;[26] since then, DNA has been an invaluable tool for criminal investigations.[27] Today, the federal government and most states have legislation regarding the collection of DNA, with a focus on DNA collection from convicted felons.[28] While states may vary the extent to which they choose to legislate on this issue, all states share their DNA information with a national database, the FBI Laboratory's Combined DNA Index System (CODIS).[29] CODIS is typically the first stop for law enforcement when trying to identify a suspect using crime scene DNA.[30] Where CODIS fails to turn up a match, as was the case with the Golden State Killer, law enforcement typically finds itself at a dead end.[31] This is where public genealogy databases like GEDmatch come in. This new type of open-source DNA database is similar to CODIS in that it contains a repository of identified DNA profiles.[32] But unlike CODIS, DNA profiles stored in this new type of public DNA database are not subject to the same regulations and protections.[33] To understand the privacy implications associated with law enforcement searches of these public genealogy databases, it is first important to understand the differences between CODIS and public genealogy databases like GEDmatch.

A. CODIS

In 1994, Congress passed the DNA Identification Act, authorizing the FBI to create a national DNA database of convicted

26. Ronald J. Rychlak, *DNA Fingerprinting, Genetic Information, and Privacy Interests*, 48 TEX. TECH. L. REV. 245, 245 (2015).
27. *Id.* at 246.
28. *Id.* at 246–47.
29. *Id.*
30. John K. Roman, *Privacy Questions Behind Catching Suspected Golden State Killer*, THE HILL (May 2, 2018, 6:30 PM), https://thehill.com/opinion/criminal-justice/385928-public-data-helped-catch-suspected-golden-state-killer-but-raises [https://perma.cc/2BZF-EXSG].
31. *Id.*
32. *Id.*
33. *Id.*

offenders as well as separate databases for missing persons and forensic samples collected from crime scenes.[34] CODIS is the resulting database, which combines all three authorized databases and enables federal, state, and local forensic laboratories to exchange and compare DNA profiles electronically, thereby linking serial violent crimes to each other and to known offenders.[35] "[A]ll fifty states currently have legislation requiring that DNA profiles of certain categories of individuals be included in at least two levels of CODIS, [but] the legislation varies from state to state concerning which classes of offenders are incorporated into the national database."[36] In 2000, with the enactment of the DNA Analysis Backlog Elimination Act,[37] Congress attempted to combat these inconsistencies by authorizing grants to the states for expanding the CODIS database to include samples taken from individuals convicted of qualifying offenses as determined by the state.[38] These offenses include convictions of murder, manslaughter, sexual abuse, child abuse, kidnapping, robbery, burglary, or any attempt or conspiracy to commit these crimes.[39] The more samples in the database, the greater the value of DNA testing in criminal investigations, hence the need to incentivize the expansion of CODIS.[40] Today, CODIS contains over 14,000,000 offender profiles, 3,700,000 arrestee profiles, and nearly 1,000,000 forensic arrestee profiles.[41] As of October 2019, CODIS had assisted in more than 477,812 investigations.[42]

The process under CODIS is relatively straightforward: DNA is collected from a crime scene, a DNA profile of the suspect is developed, and the forensic unknown suspect profile is searched against the state database of convicted offender and arrestee profiles contained within the Convicted Offender or Arrestee Index.[43] If there is a match in one of the indices, the laboratory will go through procedures to confirm the match and, if confirmed, will obtain the identity of the suspected perpetrator.[44] The match of the

34. 34 U.S.C. § 12592 (2018) (effective 1994).

35. *Combined DNA Index System (CODIS)*, FBI, https://www.fbi.gov/services/laboratory/biometric-analysis/codis [https://perma.cc/4PX4-YMYD].

36. Natalie A. Bennett, *Medical and Genetic Privacy: A Privacy Review of DNA Databases*, 4 J.L. POL'Y FOR INFO. SOC. 821, 826 (2009).

37. 42 U.S.C. § 14135 et seq.

38. *Id.*

39. *See id.*

40. Rychlak, *supra* note 26, at 246.

41. *See CODIS-NDIS Statistics*, FBI, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics [https://perma.cc/S9EQ-RSR9] (last visited Jan. 2, 2020).

42. *Id.*

43. *Frequently Asked Questions on CODIS and NDIS*, FBI, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet [https://perma.cc/J5CK-KNJ8] (last visited Jan. 2, 2020).

44. *Id.*

forensic DNA record against the DNA record in the database may be used to establish probable cause to obtain an evidentiary DNA sample from the suspect.[45] The casework laboratory can then perform a DNA analysis on the known biological sample so that this analysis can be presented as evidence in court.[46] The DNA profile of the known biological reference sample is also searched against the state's database of crime scene DNA profiles called the Forensic Index.[47] If there is a candidate match in the Forensic Index, the laboratory goes through the confirmation procedures and, if confirmed, the match will have linked two or more crimes together.[48] The law enforcement agencies involved in these cases are then able to share the information obtained in each of the cases and possibly develop additional leads.[49]

The DNA matching process described above has been found not to constitute an unconstitutional invasion of privacy because the profiles in CODIS are limited in what they reveal about a person and do not include other personal identifiers such as names.[50] A DNA profile in CODIS is created by analyzing the DNA from thirteen specific regions, or loci, of a genome.[51] Genetic variability is expressed by differing numbers of repeated sequences of DNA called short tandem repeats ("STRs").[52] Testing for identification involves comparing the genetic profiles of two samples to see if there is a match.[53] If the profiles do not match perfectly, the samples came from different sources; if they match all thirteen loci, it's almost certain that they originated from the same source.[54] When considering the privacy interests at play, the U.S. Supreme Court reasoned that the method of analyzing DNA from the thirteen loci does "not intrude on [an individual's] privacy in a way that would make his DNA identification unconstitutional" because "the CODIS loci come from noncoding parts of the DNA that do not reveal the genetic traits of the arrestee."[55]

45. *Id.*
46. *Id.*
47. *Id.*
48. *Id.*
49. *Id.*
50. *Id.*
51. Sonia M. Suter, *All in the Family: Privacy and DNA Familial Searching*, 23 HARV. J.L. & TECH. 309, 314 (2010).
52. *Id.*
53. *Id.* at 314–15.
54. *Id.* at 315; *see* Henry T. Greely et al., *Family Ties: The Use of DNA Offender Databases to Catch Offenders' Kin*, 34 J.L. MED. & ETHICS 248, 250 (2006).
55. Maryland v. King, 569 U.S. 435, 464–65 (2013).

CODIS has also been used to facilitate familial searching,[56] which is more problematic. Familial searching is used where a search turns up a partial match (meaning some, but not all, of the thirteen loci were a match).[57] A partial match suggests that "a close biological relative of the individual whose DNA partially matches the crime scene may have been the source."[58] A close match might also mean nothing of the sort because unrelated people can have some of the same genetic markers.[59] Currently, FBI policy prohibits searches of CODIS with the intent of discovering a familial match, but such searches can still be made in state or local databases.[60] Familial searches, which include the search method used to capture the Golden State Killer, are an additional problem when it comes to law enforcement use of public genealogy databases,[61] but are beyond the scope of this Note.

B. Direct-to-Consumer Genetic Testing

Despite the expansion of CODIS, an individual must have, at the very least, been arrested for a qualifying crime in order for their DNA to be collected and stored in CODIS.[62] The collection of the general public's genetic information has never been authorized, but the advent of public genealogy websites has created a secondary, public DNA database that law enforcement has quickly taken advantage of. Direct-to-consumer (DTC) genetic testing companies add to the number of DNA profiles potentially available to law enforcement, with the number of customers reaching the tens of millions.[63] These databases lack much of the oversight of CODIS and

56. *See* Suter, *supra* note 51, at 311–12 (familial searches raise additional privacy concerns by exposing innocent relatives to life-long surveillance and possible surreptitious collection of DNA simply because they are related to someone in the national database and threaten to exacerbate underlying racial inequities reflected in disproportionate rates of arrest and conviction among some minority communities).

57. *Id.* at 319.

58. *Id.*

59. *Id.*

60. SARA DEBUS-SHERRILL & MICHAEL B. FIELD, UNDERSTANDING FAMILIAL DNA SEARCHING: POLICIES, PROCEDURES, AND POTENTIAL IMPACT 4 (June 2017).

61. *See generally* Natalie Ram et al., *Genealogy Databases and the Future of Criminal Investigations*, SCIENCE (June 8, 2018), https://science.sciencemag.org/content/360/6393/1078/tab-pdf [https://perma.cc/FD57-WVJF] (providing an in-depth look at familial searching and public genealogy databases).

62. *See DNA Arrestee Laws*, NAT'L CONF. ST. LEGISLATURES, http://www.ncsl.org/Documents/cj/ArresteeDNALaws.pdf [https://perma.cc/7NNJ-QGCE].

63. *See About Us,* 23ANDME, https://mediacenter.23andme.com/company/about-us [https://perma.cc/S6XU-XYNT] ("23andMe has more than 10,000,000 customers."); *Ancestry Surpasses 5 Million People in DNA Database, Giving Customers Even More Opportunities to Discover Who They Are and How They Connect to One Another*, ANCESTRY (Aug. 9, 2017), https://www.ancestry.com/corporate/newsroom/press-releases/ancestry-surpasses-5-million-people-dna-database-giving-customers-even-more

have the potential to reveal a vast amount of information about the user.

AncestryDNA is one of the top-rated DTC genetic testing companies.[63].[64] AncestryDNA is primarily used by individuals conducting research on their family history and genealogical roots and bills itself as a DNA testing service using the latest autosomal testing technology.[65] The company uses microarray-based autosomal testing, which surveys a person's entire genome at over 700,000 locations, all with a simple saliva sample.[66] This technology is more comprehensive than previous testing methods like the Y-chromosome (Y-DNA) or mitochondrial DNA (mtDNA) tests, because AncestryDNA's testing surveys a person's entire genome and covers both the maternal and paternal sides of the family tree.[67] The Y-DNA test only reflects the father-to-son path and the mtDNA test only reflects the mother-to-child path.[68] Thus, AncestryDNA maps genetic ethnicity going back multiple generations and can help identify relationships with unknown relatives through a dynamic list of possible DNA member matches.[69]

After a user submits their DNA, they may use the results to guide investigations and connect with previously unknown relatives.[70] AncestryDNA suggests that the purpose of submitting DNA to their site is primarily to discover relatives that "may have additional information, a piece of your family story to tell, or photos to share." [71] In October of 2019, the company branched out to include genetic health screening for hereditary conditions and other health concerns.[72] As their use has expanded, Ancestry and other genetic testing companies have taken steps to protect the privacy of the information within their databases, including scraping personal identifiers, but they often sell that anonymized data to researchers or

[https://perma.cc/36BH-SXND] ("The AncestryDNA database grew from 4 to 5 million in the last three months.").

64. *See The Best DNA Ancestry Test*, FORBES (Apr. 16, 2018, 11:45 AM), https://www.forbes.com/sites/forbes-finds/2018/04/16/the-best-dna-ancestry-test/#7f561d4544bf [https://perma.cc/CS73-9TYW].

65. *AncestryDNA – Frequently Asked Questions,* ANCESTRY, https://www.ancestry.com/dna/en/legal/us/faq#about-1 [https://perma.cc/JDL2-BJT7] [hereinafter *FAQs*] (Ancestry provides more detailed information on the differences between these DNA tests on its website); *see Y-DNA, mtDNA, and Autosomal DNA Tests*, ANCESTRY, https://support.ancestry.com/s/article/Y-DNA-mtDNA-and-Autosomal-DNA-Tests [https://perma.cc/8NNA-PQEJ] [hereinafter *Tests*].

66. *FAQs*, *supra* note 65.

67. *Id.*

68. *Id.*

69. *Id.*

70. *Id.*

71. *Id.*

72. Megan Molteni, *Ancestry Branches Out into Genetic Health Screening*, WIRED (Oct. 15, 2019, 9:00 AM), https://www.wired.com/story/ancestry-branches-out-into-genetic-health-screening [https://perma.cc/4FMM-UVCG].

drug companies.[73] Ancestry's policy states that "valid legal process" is required for them to provide information to law enforcement.[74] Ancestry also offers transparency reports detailing the law enforcement requests they received, responded to, or refused.[75] Despite these protective measures, what happens when the genetic information leaves the walls of that DTC website is less clear.[76]

C. GEDmatch: The Creation of a Public Genealogy Database

One way that the DNA information generated by a site like AncestryDNA can get into the wrong hands is when an individual takes their private, non-anonymous data and submits it to a public genealogy database like GEDmatch.[77] The problem with DTC ancestry services like AncestryDNA is that the results can only link users to others who have taken the AncestryDNA test.[78] Therefore, if a relative submits their DNA to another site, such as FamilyTreeDNA,[79] a user on AncestryDNA would not get a match. The solution to this problem came in the form of GEDmatch, which was founded in 2010.[80]

GEDmatch developed as a free repository where people could upload their raw ancestry or health data from different genetic-testing services for comparison, increasing the likelihood of finding a familial match.[81] The site can estimate how close or distant the relationship is and can predict characteristics like ethnicity.[82] Law

73. Erin Brodwin, *After You Spit into a Tube for a DNA Test Like 23andMe, Experts Say You Shouldn't Assume Your Data Will Stay Private Forever*, BUS. INSIDER (Feb. 16, 2019, 7:05 AM), https://www.businessinsider.com/privacy-security-risks-genetic-testing-23andme-ancestry-dna-2019-2 [https://perma.cc/N5SC-DZWQ]; *see* Julian Segert, *Understanding Ownership and Privacy of Genetic Data*, HARV. U. SCI. IN THE NEWS BLOG (Nov. 28, 2018), http://sitn.hms.harvard.edu/flash/2018/understanding-ownership-privacy-genetic-data [https://perma.cc/44XW-DGSJ].

74. *See Ancestry Guide for Law Enforcement*, ANCESTRY, https://www.ancestry.com/cs/legal/lawenforcement [https://perma.cc/Q8SU-Q26W].

75. *Ancestry 2018 Transparency Report*, ANCESTRY, https://www.ancestry.com/cs/transparency-2018 [ttps://perma.cc/Y865-ASRN] (Ancestry's 2018 transparency report reveals that out of ten valid law enforcement requests in 2018, they provided information in response to seven of those requests and all related to investigations involving credit card misuse, fraud, and identity theft).

76. Brodwin, *supra* note 73.

77. *Id.*

78. *FAQs*, *supra* note 65.

79. *See generally* FAMILYTREEDNA, https://www.familytreedna.com [https://perma.cc/9A6T-XK3D].

80. Heather Murphy, *How and Unlikely Family History Website Transformed Cold Case Investigations*, N.Y. TIMES, https://www.nytimes.com/2018/10/15/science/gedmatch-genealogy-cold-cases.html [https://perma.cc/Z4RB-V76N].

81. Dina Fine Maron, *Cold Cases Heat Up as Law Enforcement Uses Genetics to Solve Past Crimes*, SCI. AM. (July 2, 2018), https://www.scientificamerican.com/article/cold-cases-heat-up-as-law-enforcement-uses-genetics-to-solve-past-crimes [https://perma.cc/633F-PBYU].

82. *Id.*

enforcement soon discovered GEDmatch's potential as an investigative tool–by converting crime scene DNA to the kind of profile that sites such as AncestryDNA are built on and uploading that information to GEDmatch, law enforcement is able to find their suspect or relatives of the suspect and narrow down their list from there.[83] In 2018, an estimated two-hundred cases were investigated using this method after the method proved successful in the Golden State Killer investigation.[84] In "many of those cases, officers never sought a warrant or any legal process at all," the argument being that people using public genealogy sites have no expectation of privacy in their genetic data because they have willingly shared that data with a third party.[85]

After law enforcement revealed their use of GEDmatch to identify the Golden State Killer, the company embraced the use of its database by law enforcement.[86] GEDmatch's policy "allowed investigators to pursue leads on homicides and rapes, but not less serious crimes."[87] The difficulty in this self-monitoring policy soon became apparent. The company bent its own rules in at least one instance, allowing law enforcement to search for the suspect of a violent assault.[88] The decision to ignore its own policy ignited a backlash against the company, and on May 18, 2019, GEDmatch changed its terms of service to add a privacy setting whereby users may opt out from having their profiles made available for warrantless searches by police.[89] The decision instantly limited law enforcement's access to information in GEDmatch's database.[90] While this seemed promising from a privacy protection standpoint, another major change in 2019 could spell greater danger. On December 9, 2019, GEDmatch was acquired by Verogen, a for-profit forensic genomics company with a clear goal of using GEDmatch as a crime-fighting tool.[91]

Today, GEDmatch contains the genetic information of over 1.3 million users and a study found that from that information, the

83. *Id.*
84. *Id.*
85. *Id.*
86. Jon Schuppe, *Police Were Cracking Cold Cases with a DNA Website. Then the Fine Print Changed*, NBC NEWS (Oct. 23, 2019, 5:19 PM), https://www.nbcnews.com/news/us-news/police-were-cracking-cold-cases-dna-website-then-fine-print-n1070901 [https://perma.cc/ZR5R-TD9N].
87. *Id.*
88. *Id.*
89. *Id.*
90. *Id.*
91. Nila Bala, *We're Entering a New Phase in Law Enforcement's Use of Consumer Genetic Data*, SLATE: FUTURE TENSE (Dec. 19, 2019, 7:30 AM), https://slate.com/technology/2019/12/gedmatch-verogen-genetic-genealogy-law-enforcement.html [https://perma.cc/RNU4-E2BR].

identities of over 60% of white Americans can be determined.[92] The uncertainty in how this treasure trove of genetic information will be handled illustrates the need for clear guidelines for law enforcement. It also speaks to the need for a deeper understanding of how this highly sensitive and uniquely private information can best be protected while respecting law enforcement's investigative needs.

II. THE DEVELOPMENT OF THE THIRD-PARTY DOCTRINE: HOW WE GOT HERE

The Fourth Amendment establishes "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[93] The approach to a search within the meaning of the Fourth Amendment was largely property-based until *Katz v. United States*.[94] In *Katz*, the Supreme Court established that the Fourth Amendment "protects people, not places."[95] Justice John Marshall Harlan's concurring opinion in *Katz* formulated what is now known as the Fourth Amendment's "reasonable expectation of privacy" test.[96] The *Katz* test is used to determine when a governmental intrusion constitutes a "search" under the Fourth Amendment. The two-prong test first asks whether an individual had a subjective expectation of privacy in the information, and then whether that expectation of privacy is one that "society is prepared to recognize as 'reasonable.'"[97] If there is no expectation of privacy, then there is no "search" under the Fourth Amendment, and therefore no Fourth Amendment violation.[98] Later cases would establish the third-party doctrine, which says that a person cannot have a reasonable expectation of privacy in information disclosed to a third party.[99] Categorically applying this understanding of the third-party doctrine to searches of public genealogy websites would mean that all privacy interests are lost in the genetic information a user submits to one of these sites. However, a deeper look at the development of the third-party doctrine

92. *Id.*; Yaniv Erlich et al., *Identity Inference of Genomic Data Using Long-Range Familial Searches*, SCIENCE (Nov. 9, 2018), https://science.sciencemag.org/content/362/6415/690/tab-pdf [https://perma.cc/5TRJ-7SYD].

93. U.S. CONST. amend. IV.

94. Trevor Burrus & James Knight, *Katz Nipped and Katz Cradled: Carpenter and the Evolving Fourth Amendment*, 2017–2018 CATO SUP. CT. REV. at 79, 83 (2018), https://www.cato.org/sites/cato.org/files/serials/files/supreme-court-review/2018/9/2018-cato-supreme-court-review-4.pdf [https://perma.cc/UYU3-GCCY].

95. Katz v. United States, 389 U.S. 347, 351 (1967).

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

97. *Id.*

98. *Id.*

99. *See* Kerr, *supra* note 15, at 563; *see also* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

and a close reading of the recent U.S. Supreme Court case, *Carpenter v. United States*, offers an alternative view that could afford that information protection despite the voluntary submission of the information to a third-party.

A. Early Cases

Throughout the 1970s, the Supreme Court established the third-party doctrine as a mainstay of Fourth Amendment jurisprudence, finding no reasonable expectation of privacy in records given to an accountant[100] or in records given to a bank.[101] The Court consistently reasoned that by revealing information to a third party, that person takes the risk that the information will be conveyed to the government, "[e]ven if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[102]

The heart of the third-party doctrine was established in *United States v. Miller* in 1976.[103] In that case, the government subpoenaed banks used by the defendant Miller seeking all records of his accounts.[104] The U.S. Supreme Court ultimately held that subpoenaing the bank records without a warrant did not violate the Fourth Amendment for two reasons: (1) the bank records were financial documents that would be used in the ordinary course of business and thus not of a private or personal nature[105] and (2) the defendant had voluntarily conveyed the information to a third party.[106] In his majority opinion, Justice Powell articulated the meaning of the third-party doctrine, reiterating the Court's past holdings that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[107]

Three years after *Miller*, the Supreme Court solidified the third-party doctrine in *Smith v. Maryland*. [108] There, the Supreme Court held that the Fourth Amendment does not apply to the numbers dialed on a telephone.[109] In *Smith v. Maryland*, when police

100. *See* Couch v. United States, 409 U.S. 322, 335 (1973).
101. *See* United States v. Miller, 425 U.S. 435, 442–43 (1976).
102. *Id.* at 443.
103. *See id.*
104. *Id.* at 435.
105. *Id.* at 442.
106. *Id.* at 443.
107. *Id.*
108. *See* Smith v. Maryland, 442 U.S. 735 (1979).
109. *Id.*

suspected that the defendant was making threatening phone calls to a robbery victim, they asked the phone company to install a "pen register." [110] A pen register is a surveillance tool that discloses the phone numbers that have been dialed from a telephone.[111] The information from the pen register was used to show that the calls to the victim were originating from the phone in the defendant's apartment.[112] The defendant moved to suppress the evidence, arguing that the Fourth Amendment protected the numbers he dialed from his phone.[113] But the *Smith* Court concluded that when he dialed the numbers from his phone, the defendant was voluntarily disclosing the information to the phone company.[114] The Court felt that the defendant could not have a subjective expectation of privacy in the numbers he dialed because people generally know that they must convey dialed numbers in order to complete a call and that phone companies record those numbers.[115] The Court continued that even if the defendant had an expectation of privacy, it was not one society was prepared to recognize as reasonable.[116]

In making the reasonableness determination, the Court applied the straightforward principle of the third-party doctrine: because the defendant had voluntarily conveyed the telephone numbers, he'd exposed that information to the company and could not reasonably expect privacy in that information and had thus "assumed the risk" that the company would reveal that information to law enforcement.[117] In his dissenting opinion, Justice Marshall offered an early critique of the third-party doctrine, questioning the *Smith* majority's view that privacy was disclosed to all when it was disclosed to one.[118] Justice Marshall reasoned "[p]rivacy is not a discrete commodity, possessed absolutely or not at all."[119] He continued, "those who disclose certain acts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[120] Justice Marshall suggested that the question of an individual's legitimate expectation of privacy should not be about "the risks an individual can be presumed to accept when imparting information

110. *Id.* at 737.
111. *Id.* at 741.
112. *Id.* at 737.
113. *Id.* at 737–38, 743–44.
114. *Id.* at 743–44.
115. *Id.* at 742.
116. *Id.* at 743.
117. *Id.* at 744.
118. *See id.* at 749 (Marshall, J., dissenting).
119. *Id.*
120. *Id.*

to third parties, but on the risks he should be forced to assume in a free and open society."[121]

The application of the third-party doctrine to the phone numbers one dials (as in *Smith*) or the checks and deposits one gives to their bank (as in *Miller*) is based on the straightforward premise that because the individual exposed that information to a third party, they have assumed the risk that the information could be handed over to the government. But technology and society have advanced at a rapid pace since the advent of the third-party doctrine, bringing the practicality of the doctrine into question. Determining when a person has assumed the risk is made difficult by the fact that we now live in a society which increasingly "shares almost every facet of its life with various entities."[122]

B. Carpenter v. United States: A Twenty-First Century Look at the Third-Party Doctrine

In *Carpenter v. United States*, the Supreme Court took its first serious look at the third-party doctrine in relation to our technologically advanced society, considering the government's collection of an individual's cell-site location information ("CSLI") data.[123] Cell phones continuously search for the cell site providing the best signal, and when a connection is made a time-stamped record indicating the location of the cell phone and the time of connection is generated.[124] In *Carpenter*, the Supreme Court considered whether the government's collection of defendant Carpenter's CLSI was a search under the Fourth Amendment.[125] Under existing third-party doctrine precedent, it seemed likely that the Court would rule against Carpenter. But the Court held the opposite, and in doing so has opened the door to a new understanding of the third-party doctrine.

The issue in *Carpenter* arose in the context of a federal investigation into a series of robberies.[126] One of the men involved in the robberies confessed and identified his accomplices; the FBI then reviewed call records to identify additional numbers he had called around the time of the robberies.[127] Based on that information, law

121. *Id.* at 750.
122. RICHARD M. THOMPSON II, CONG. RESEARCH SERV., THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE 2 (2014), https://fas.org/sgp/crs/misc/R43586.pdf [https://perma.cc/KN5L-DN8C].
123. Carpenter v. United States, 138 S. Ct. 2206, 2206 (2018).
124. Carpenter v. United States, No 16-402, slip op. at 1, 138 S. Ct. 2206 (2018).
125. *Id.* at 2213.
126. *Id.* at 2212–13.
127. *Id.* at 2212.

enforcement sought and obtained Carpenter's CSLI.[128] Carpenter's CSLI data provided the government with the incoming and outgoing calls on Carpenter's cell phone during the four-months when the string of robberies occurred.[129] Altogether, the government obtained 12,898 location points cataloging Carpenter's movements, which showed that Carpenter's phone was near four of the robberies.[130] Carpenter was charged with six counts of robbery and six counts of carrying a firearm during a federal crime of violence.[131] Carpenter moved to suppress the CSLI data, arguing that the government had violated the Fourth Amendment because they seized the CSLI records without a warrant supported by probable cause but his motion was denied.[132] Carpenter was convicted; and the conviction was subsequently confirmed by the Court of Appeals for the Sixth Circuit.[133]

The Supreme Court saw the issue of whether the location information was private as lying "at the intersection" of (1) cases holding that a person had a reasonable expectation of privacy in their physical location and movements, and (2) cases applying the third-party doctrine.[134] For the purposes of this Note, I focus solely on the Court's third-party doctrine analysis. Ultimately, the Court declined to extend the third-party doctrine to cover cell site information and reversed Carpenter's convictions. In reversing Carpenter's conviction, the *Carpenter* Court explicitly declined to extend Fourth Amendment precedent to cover historic cell site information.[135] Departing from the concrete rule of *Smith* and *Miller* that an individual has no legitimate expectation of privacy in information he voluntarily turns over to third parties,[136] the *Carpenter* Court reasoned that "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment privacy."[137] Rather, the Court's analysis leaves room to argue that there is now an additional layer of inquiry to conduct before the third-party doctrine can be implicated—the nature of the

128. *Id.*
129. *Id.* at 2212–13.
130. *Id.*
131. *Id.* at 2212.
132. *Id.*
133. *Id.* at 2213 (in a strict application of the third-party doctrine, the Sixth Circuit held that Carpenter lacked a reasonable expectation of privacy in the location information collected by the FBI because he had shared that information with his wireless carriers. Given that cell phone users voluntarily convey cell-site information to carriers in order to establish communication, the Court ruled that the records were not entitled to Fourth Amendment protection).
134. *Id.* at 2214–15.
135. *Id.* at 2217.
136. *See* United States v. Miller, 425 U.S. 435 (1976); *see also* Smith v. Maryland, 442 U.S. 735 (1979).
137. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

information held by the third party and the voluntariness of the information's exposure.[138]

The *Carpenter* Court distinguished the case from *Smith* and *Miller* in two important ways. First, the Court considered the "revealing nature" of CSLI as compared to the limited capabilities of the pen register in *Smith* and the nature of the checks as negotiable instruments in *Miller*.[139] Second, the Court considered whether there was truly a "voluntary exposure" of information when it comes to CSLI.[140] The Court held that because having a cell phone is "indispensable to participation in modern life" and because CSLI is recorded without any affirmative act on part of the user, the user has not voluntarily assumed the risk of turning over a "comprehensive dossier of his physical movements".[141]

Chief Justice Roberts, writing for the majority, insisted that the holding was a narrow one, but the implications of the decision have far-reaching potential nonetheless.[142] Holding that "a warrant is required in the rare case where the suspect has a legitimate privacy interest in records held by a third-party" the Court has departed from the categorical rule of *Smith* and *Miller* that where information is held by a third party, there is no privacy interest at all.[143]

III. GOVERNMENT SEARCHES OF DNA DATABASES AND THE THIRD-PARTY DOCTRINE POST-CARPENTER

Dissenting in *Carpenter*, Justice Gorsuch asked: "Can [the government] secure your DNA from 23andMe without a warrant or probable cause? *Smith* and *Miller* say yes it can—at least without running afoul of *Katz*." [144] Gorsuch seems to suggest that the majority's decision in *Carpenter* adds nothing to this analysis, but that may be too quick of a dismissal. In this section, I propose that *Carpenter* has added an additional layer of inquiry to the third-party doctrine. I then apply that test to warrantless government searches of public DNA databases, specifically GEDmatch.

A. The Carpenter Test

Prior to *Carpenter*, the third-party doctrine simply meant that wherever an individual had voluntarily given information to a third

138. *See id.*
139. *Id.* at 2219.
140. *Id.* at 2220.
141. *Id.*
142. *Id.*
143. *Id.* at 2262 (Gorsuch, J., dissenting).
144. *Id.* at 2262 (Gorsuch, J., dissenting).

party, they gave up their reasonable expectation of privacy in that information. But the majority opinion in *Carpenter* is more protective of privacy even where that information is held by a third party, particularly with today's technological advancements.[145] *Carpenter* holds that one does not automatically lose their expectation of privacy (and therefore Fourth Amendment protection) just because their information is now held by a third party.[146] Instead, a court must first look at whether there is a legitimate privacy interest in the information at issue.[147] This inquiry appears to be highly fact specific. It focuses on the nature of the information and whether there was truly a voluntary exposure of the information to a third party.[148] If, after conducting this inquiry, a court determines that the individual had a legitimate privacy interest in that information, then the fact that it is now held by a third party does not automatically defeat that individual's expectation of privacy and may still be a Fourth Amendment search.[149] If, on the other hand, the court finds that there is no legitimate privacy interest and instead the information is more like that of *Miller* or *Smith*, then the traditional view of the third-party doctrine still applies.[150] In *Carpenter*, the Court found that there was a legitimate privacy interest in the CSLI data.[151]

1. Nature of the Information

Looking at the nature of the information, Chief Justice Roberts determined that the nature of CSLI is "deeply revealing" and involved significant "depth, breadth, and comprehensive reach."[152] This was not the case in *Miller*, where the nature of the bank records were not those of confidential communications, but rather "negotiable instruments to be used in commercial transactions."[153] Similarly, the *Carpenter* Court was able to distinguish the nature of the CSLI information from that of the pen register in *Smith*.[154] Unlike the ability of CSLI to completely "chronicle a person's past movements through the record of his cell phone signals," pen registers had limited capabilities and a telephone subscriber would

145. *Id.* at 2219 ("The government's position fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years.").
146. *Id.* at 2220.
147. *Id.* at 2219.
148. *Id.* at 2219–20.
149. *Id.* at 2219.
150. *Id.* at 2216.
151. *Id.* at 2216–17.
152. *Id.* at 2223.
153. *Id.* at 2216.
154. *Id.*

presumably be aware that the numbers they dial are used by the telephone company.[155] The nature of the pen register information differs from that of CSLI when it comes to an individual's expectations of privacy because, as Chief Justice Roberts explicitly stated, "when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements."[156] The majority thus based its decision on whether the defendant maintained a privacy interest in his CLSI data not on *who* held the information, but because of *what* that information revealed.

2. Voluntariness of Exposure

Turning to the voluntariness of the exposure, the *Carpenter* Court reasoned that "cell phone location information is not truly 'shared' as one normally understands the term."[157] The Court focused on the fact that the use of cell phones is almost mandatory if one wishes to participate actively in today's society.[158] Further, generating CSLI data is an involuntary act—unless one affirmatively disconnects their phone, the phone is always generating CSLI and leaving a trail of location data.[159] Chief Justice Roberts held that as a result of this automatic collection, "in no meaningful sense does the user voluntarily 'assume the risk' of turning over a comprehensive dossier of his physical movements."[160]

B. Kerr's Equilibrium Adjustment Theory

This reading of *Carpenter* is best understood with Fourth Amendment scholar Professor Orin Kerr's equilibrium-adjustment theory in mind.[161] Professor Kerr's theory is that the "Supreme Court often engages in equilibrium adjustment when new technology threatens the balance of government power."[162] If technology gives the government too much new power so that it can be abused based on old rules, the Court expands legal protection to restore old levels of power and limit abuses.[163] Alternatively, if technology

155. *Id.*
156. *Id.* at 2217.
157. *Id.* at 2210.
158. *Id.*
159. *Id.* at 2220.
160. *Id.*
161. Orin Kerr, *First Thoughts on Carpenter v. United States*, VOLOKH CONSPIRACY (June 22, 2018, 12:20 PM), https://reason.com/volokh/2018/06/22/first-thoughts-on-carpenter-v-united-sta [https://perma.cc/ES2E-VUTK].
162. *Id.*
163. *Id.*

threatens to narrow government power so much that it unduly limits the government's ability to solve crimes under old rules, the Court shrinks legal protection to restore old levels of power and ensure the government can still solve enough cases.[164]

To read *Carpenter* in the equilibrium-adjustment theory's framework, the majority essentially determined that new technology (in that case, CSLI) granted the government too much power that it could then abuse based on old rules (the third-party doctrine). As a result, the Court was inclined to expand the legal protection. According to Kerr's reading of the *Carpenter* opinion, the Court adopted the idea that the third-party doctrine does not entirely eliminate an expectation of privacy, it just diminishes it.[165] The balance in *Carpenter* was tipped in favor of more power for the government with technology that is vastly more revealing and sensitive than records considered in previous third-party doctrine cases like *Smith* and *Miller*.[166]

This reading of *Carpenter* makes sense, particularly because of the Court's insistence that its holding leaves the third-party doctrine of *Smith* and *Miller* intact in all but unique instances. In justifying its categorization of CSLI as one type of the information that should be afforded greater protection, the *Carpenter* Court reiterates the importance of considering the new technology available and its desire to avoid a categorical application of old rules that would give the government too much power.[167]

C. An Individual's Privacy Interest in Their DNA

The *Carpenter* Court insisted that its holding was narrow and declined to consider how its holding might apply to other types of information.[168] But reading *Carpenter* through the lens of the equilibrium-adjustment theory, an argument can be made that one's DNA is precisely the kind of unique information that deserves the privacy protections *Carpenter* afforded to CSLI. This section demonstrates how *Carpenter* might be used to protect one's genetic information held by a third party. In doing so, this section imagines

164. *Id.*
165. *Id.*
166. *Id.*
167. *See* Carpenter v. United States, 138 S. Ct. 2206, 2222–23 (2018). ("Here the progress of science has afforded law enforcement a powerful new tool to carry out its important responsibilities. At the same time, this tool risks Government encroachment of the sort the Framers, 'after consulting the lessons of history,' drafted the Fourth Amendment to prevent.") ("At some point, the dissent should recognize that CSLI is an entirely different species of business record—something that implicates basic Fourth Amendment concerns about arbitrary government power much more directly than corporate tax or payroll ledgers. When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents.").
168. *Id.* at 2220.

a case where law enforcement, without a warrant, has uploaded unknown crime scene DNA to a public genealogy database like GEDmatch. For purposes of this analysis, this section considers an individual's Fourth Amendment rights where they have personally uploaded their genetic information to seek out their family history. This individual ("John Doe") is now being charged with murder after law enforcement matched the unknown crime scene DNA to the John Doe's DNA in GEDmatch. Relying on *Carpenter*, John Doe now argues he has a legitimate privacy interest in his DNA despite having given it to a third-party. John Doe argues that law enforcement's act was a Fourth Amendment search that violated his reasonable expectation of privacy. Putting John Doe's case to the test under the new *Carpenter* framework, a court would need to determine if John Doe has a legitimate expectation of privacy in the DNA information he has uploaded to GEDmatch. This determination involves considering the nature of the information and the voluntariness of the exposure.

1. Nature of the Information

DNA is much like CSLI in the sense that it reveals so much information about an individual. If the *Carpenter* Court was concerned that CSLI data provides the government with an intimate portrait of human life,[169] then the same concern should be heightened when it comes to DNA information. DNA is an "information-containing blueprint of human life, revealing one's genetic predisposition to disease, physical and mental characteristics, and a host of other private facts not evident to the public."[170] While this is true of the DNA information stored in CODIS, it is especially true when it comes to the DNA available in public genealogy databases. DTC genetic testing services like AncestryDNA and 23andMe are the source of the DNA information that is then uploaded by the user to a public genealogy database like GEDmatch. CODIS does not store the whole DNA sequence, but DTC genetic testing services do, providing "single-letter variations in DNA across hundreds of thousands of sites in the human genome."[171] These additional data points allow a more accurate assessment of a person's relationship with others and reveal a whole host of additional information.[172]

169. *Id.* at 2217.

170. Mark A. Rothstein & Sandra Carnahan, *Legal and Policy Issues in Expanding the Scope of Law Enforcement DNA Data Banks*, 67 BROOK. L. REV. 127, 156 (2002).

171. Chelsea Whyte, *Police Can Now Use Millions More DNA to Find Criminals*, NEWSCIENTIST (Oct. 11, 2018), https://www.newscientist.com/article/2182348-police-can-now-use-millions-more-peoples-dna-to-find-criminals [https://perma.cc/5VFH-6VZF].

172. *Id.*

Unlike the CODIS system, which intentionally does not reveal information beyond genetic identity, DTC genetic testing service data can reveal physical or medical characteristics.[173] The increase in information means that there is an increased risk to privacy. Regardless of where the information is stored, a court should find that the nature of the information is inherently revealing, and thus more like the CSLI data in *Carpenter* than the bank records in *Miller* or the pen register in *Smith*.

2. Voluntary Exposure of the Information

In *Carpenter*, the Court emphasized the automatic collection of CSLI as tending to show that the user had not voluntarily put their information in the hands of a third-party.[174] There is no doubt that the act of acquiring one's DNA information from DTC genetic testing services and then uploading that DNA to a public genealogy database is voluntary. But *Carpenter* does not mention the weight of either the nature of the information or the voluntariness of the exposure should be given.[175] Thus, since the nature of one's genetic information is so much more revealing (it is essentially a dataset detailing one's entire self), perhaps the level of voluntariness should not completely defeat protection.

The unique qualities of genetic data and the extent of the information it is capable of sharing offer one way to look at the voluntary exposure prong. Even if an individual has voluntarily submitted *their* genetic information to a public genealogy database, it could be argued that they are not voluntarily submitting *their relative's* DNA to the potential exploitation by law enforcement. The problem is that this is so difficult to separate and much like the only way to avoid generating CSLI data in *Carpenter* is to avoid using a cell phone,[176] the only way to avoid generating a list of potential suspects of your family members is to avoid submitting DNA at all. While researching one's family history is not quite the necessity of day to day life as using a cell phone is, individuals arguably should not have to make the choice between finding their long-lost relatives or subjecting themselves, and more importantly their unsuspecting family members, to warrantless government searches.

Further, individuals uploading their genetic information to sites like GEDmatch typically do so with the intention of researching their ancestry, not for helping law enforcement. This argument is supported by GEDmatch's recent change to its terms of service, which now requires users to opt in to sharing profiles with law

173. *Id.*
174. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).
175. *See id.*
176. *Id.* at 2220.

enforcement. Additionally, the collection of DNA housed in public genealogy websites arguably is becoming automatic. In the years since genealogy testing services like 23andMe and Ancestry.com have come on the scene, more than 15 million people have offered up their DNA in the pursuit of genetic answers. As a result, a study has revealed that 60% of Americans of Northern European descent can now be identified through such databases regardless of whether or not they have joined one themselves. The researchers determined that a genetic database needs to cover only 2% of the target population to provide a third-cousin match to nearly any person. The expansiveness of this new technology means that where the act may be voluntary for some, it is not voluntary for all. Privacy concerns should favor protecting genetic information for this reason alone. Indeed, the idea of a forward-looking approach to what the new technology could mean, as opposed to what it means now, is supported by the majority in *Carpenter*: "While the records in this case reflect the state of technology at the start of the decade, the accuracy of CSLI is rapidly approaching GPS-level precision."

IV. MOVING FORWARD

Before *Carpenter*, a strict reading of the third-party doctrine meant that the genetic information one submits to a third-party public genealogy site is not given Fourth Amendment protection from warrantless government searches. After *Carpenter*, the argument could be made that one possesses a legitimate privacy interest in their genetic information, even if that information is now held by a third party. Aided by an application of Professor Orin Kerr's equilibrium-adjustment theory, I argue that *Carpenter* should be read to find a legitimate privacy interest in one's genetic information and therefore afforded Fourth Amendment protection. However, there are recognizable benefits to the use of this technology when it comes to resolving cold cases and bringing closure to families that should not be ignored. To get the most out of this new investigative method while maintaining crucial privacy protections, I suggest potential legislative and regulatory solutions.

A. Using Carpenter to Protect Genetic Privacy

The issue at the core of both *Carpenter* and searches of DNA stored in public genealogy databases is arguably the same: the blanket approach of the third-party doctrine does not make sense in today's technologically advanced world. *Carpenter* can be read to mean that one no longer automatically loses their expectation of privacy (and therefore Fourth Amendment protection) just because

their information is now held by a third party.[177] Instead, a court must first look at whether there is a legitimate private interest in the information at issue.[178] Looking at the nature of the information, a strong argument can be made that *Carpenter*'s rationale applies with equal, if not greater, force to genetic information. Like CSLI data, genetic information is "deeply revealing" and involves significant "depth, breadth, and comprehensive reach."[179] While the act of submitting one's genetic information to a public database is significantly more voluntary than the automatic collection of CSLI data, reading *Carpenter* in the lens of Professor Orin Kerr's equilibrium-adjustment theory suggests that the voluntariness of the act alone should not cause an individual to lose their legitimate privacy interest in their genetic information.

The equilibrium-adjustment theory says that if law enforcement "can easily take investigative steps that far exceed their powers in the past . . . that newfound ability violates a reasonable expectation of privacy."[180] It could be argued that law enforcement's powers in the past only included the CODIS searches, meaning that only violent offenders and arrestees were included.[181] It is reasonable to assume that an individual who was arrested or convicted of a violent crime is aware that their DNA has been entered into a database and that law enforcement can search that database. But an individual who uploaded their DNA to an ancestry site five years ago might not expect that their DNA would now be accessible in a law enforcement investigation because law enforcement has not traditionally used genealogy sites in their investigations. As Kerr argues, "new powers mean new practices, and new practices mean new expectations of those practices."[182]

Furthermore, the majority in *Carpenter* focused on how private the information actually is, regardless of who holds that information.[183] Focusing on the serious privacy interests and potentially limitless uses of DNA, a court could find that genetic information is deserving of greater privacy concerns, even if it is held by a third party.

177. *See id.* at 2220.
178. *See id.* at 2222.
179. *Id.* at 2223.
180. Orin Kerr, *Implementing Carpenter, in* THE DIGITAL FOURTH AMENDMENT (forthcoming) (manuscript at 8).
181. *See* 42 U.S.C. § 14132 (2018)*; see also* Rothstein & Carnahan, *supra* note 170, at 130–32 (discussing the statutory framework for the CODIS system).
182. Kerr, *supra* note 180, at 9.
183. *See supra* Part III.A.1.

B. Legislative Solutions

The holding in *Carpenter* has added a new dimension to the third-party doctrine, but its effect in the realm of genetic privacy is yet to be seen. Courts will inevitably face this issue, but in the meantime the legislature should act to strike the proper balance between privacy and security when it comes to genetic information.

1. Existing Privacy Laws

There are currently no general privacy laws in the United States when it comes to protecting genetic information.[184] Rather, different laws regulate genetic data depending on where it is and what it is being used for.[185] The problem with this approach is that the intended use of genetic information in one instance might not be the use that is ultimately employed.[186] Without a general law protecting genetic information, legislatures should first look to address the specific issue of genetic information from DTC genetic testing services used in law enforcement searches.

With the Stored Communications Act, Congress provided substantial statutory protection for email and other *digital communications information* maintained on the internet.[187] Under the Act, a court may order disclosure of qualifying electronic records if the government "offers specific and articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation."[188] A preliminary study showed that individuals are not particularly concerned about police searches of personal genetic data on genetic genealogy databases when that purpose is considered justified, i.e. when the purpose is to identify perpetrators of violent crimes, crimes against children, or missing persons.[189] Thus, as long as the

184. *See* Megan Molteni, *The US Urgently Needs New Genetic Privacy Laws*, WIRED (May 1, 2019), https://www.wired.com/story/the-us-urgently-needs-new-genetic-privacy-laws [https://perma.cc/2L2G-ZM35].

185. *Id.* (describing how genetic data used in a research study is governed under the 21st Century Cures Act and cannot be accessed by law enforcement, but that same genetic data in an electronic health record is personal health data governed under HIPAA, and can be accessed by law enforcement without a warrant if that person is a victim or suspect of a crime); *see* Health Insurance Portability and Accountability Act (HIPAA) (preventing personal health data in your health record from being given to your school or employer); *see* Genetic Nondiscrimination Act (GINA) (preventing health insurers from denying coverage or jacking up prices based on someone's genetic predisposition to various health conditions).

186. *See id.*

187. *See* 18 U.S.C. § 2703 (2018).

188. *Id.*

189. *See* Christi 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),

government can offer some specific and articulable facts showing that there is some link between the records in the database and an ongoing material investigation, consumers would likely not have a problem with the information being searched subject to a court order.

Enacting legislation similar to the Stored Communications Act could ensure some level of protection against unlimited genetic surveillance by law enforcement while satisfying the public's interest in having crimes solved and dangerous criminals off the streets. Legislation protecting genetic data stored in public genealogy sites would ensure that the government cannot subject ordinary individuals to genetic searches without some specific and articulable facts showing that the particular individual may be tied to a particular crime. This would limit the use of genealogy sites by law enforcement to investigating existing leads as opposed to searches in the hopes of generating leads.[190] The downside, of course, would be that the protection from perpetual genetic surveillance would likely result in fewer solved cases.[191] If legislatures do not want to risk eliminating the main benefit of searching these types of databases, at a minimum they should make clear under what circumstances such searches are acceptable.[192]

Expanding the United States' primary health privacy law, Health Insurance Portability and Accountability Act (HIPAA)[193], to cover websites like DTC genetic testing services and public genealogy databases like GEDmatch is another possibility. HIPAA currently only applies to "covered entities," which means organizations traditionally associated with healthcare.[194] HIPAA holds covered entities to a high standard of care, requiring that they maintain the confidentiality of patient data and penalizing them in the event of

https://journals.plos.org/plosbiology/article?id=10.1371/journal.pbio.2006906 [https://perma.cc/4ASE-NW7Z] ("Among the 1,587 respondents, the majority supported police searches of genetic websites that identify genetic relatives (79%) and disclosure of DTC 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%).").

190. Natalie Ram, Christi J. Guerrini & Amy L. McGuire, *Genealogy Databases and the Future of Criminal Investigation*, 360 SCI. 1078, 1079 (2018).

191. *Id.*

192. *Id.*

193. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936 (codified as amended in scattered sections of 26, 29, and 42 U.S.C.).

194. Mason Marks & Tiffany Li, *DNA Donors Must Demand Stronger Protection for Genetic Privacy*, STAT NEWS (May 30, 2018), https://www.statnews.com/2018/05/30/dna-donors-genetic-privacy-nih [https://perma.cc/CPF5-M6E6].

a data breach.[195] Expanding HIPAA to cover all companies that handle health data, which would include DTC genetic testing services, would require them to use the same privacy standards as doctors and hospitals.[196] This uniformity would benefit both consumers and the companies in providing clear standards when it comes to law enforcement searches of the genetic data they possess. Considering the highly sensitive information at stake, this method would have the added benefit of creating a level of security to limit the danger of a data breach.

2. New Solutions

In 2013, the American Bar Association's Criminal Justice Standards Committee specifically addressed the issue of law enforcement access to third party records.[197] The Committee proposed a limit on the third-party doctrine, recognizing that law enforcement's ability to access personal information via the third-party doctrine has dramatically increased, warranting greater concern for privacy.[198] With these competing interests in mind, the Committee proposed a set of standards that would "provide a framework via which they can bring greater consistency to existing law, and, where necessary, frame new law that accounts for changing technologies and social norms, the needs of law enforcement, and the interests of privacy, freedom of expression, and social participation."[199]

The Committee proposed that legislatures, courts, and administrative agencies categorize third-party information based on the level of confidentiality it deserves.[200] Types of information maintained by institutional third parties should be classified as highly private, moderately private, minimally private, or not private.[201] The Committee offers guidelines for how such determinations should be made.[202] The level of privacy corresponds to the level of

195. *Id.*

196. *Id.*

197. AMERICAN BAR ASS'N., CRIMINAL JUSTICE STANDARDS COMM., ABA STANDARDS FOR CRIMINAL JUSTICE: LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS (3d ed. 2013), https://www.americanbar.org/content/dam/aba/publications/criminal_justice_standards/third_party_access.pdf [https://perma.cc/JJR5-VULN].

198. *Id.* at 3–4 ("Of course, such law enforcement access implicates privacy. At information privacy's core is an ability to control what information about you is conveyed to others, and for what purposes. American norms of government and principles of freedom of speech and association thus require that law enforcement records access be regulated.").

199. *Id.* at 4.

200. *Id.* at 19.

201. *Id.*

202. *Id.* at 19–20. ("[A] legislature, court, or administrative agency should consider present and developing technology and the extent to which: (a) the initial transfer of

protection that should be afforded. Consistent with the law of privilege, information classified as highly private should be highly protected—law enforcement should only be permitted to access a highly protected record via a warrant supported by probable cause.[203] For moderately protected information, access should require a court order supported by reasonable suspicion or, if the legislature or other decision maker so chooses, a court order supported by relevance or issued pursuant to a prosecutorial certification.[204] Access to minimally protected information should require a prosecutorial or agency determination of relevance.[205] And access to unprotected information should be permissible for any legitimate law enforcement purpose.[206]

Under this regime, DNA information submitted to a public genealogy database would likely be categorized as either highly or moderately private. Either way, some level of court intervention is required and there is a level of clarity afforded to the consumer. Additionally, this ensures that law enforcement is not entirely foreclosed from accessing this information and restores a balance between privacy interests and law enforcement interests that has been eroded by existing third-party doctrine.

At least one state representative has moved for an outright ban on law enforcement use of genealogy databases.[207] Utah Representative Craig Hall is working with the state attorney's general office to draft legislation that would prevent mass searches of consumer DNA databases, which he views as "fishing expeditions."[208] The legislation is specifically targeted at companies like GEDmatch, citing concerns that the privacy protections the company offers are not enough.[209] Hall hopes the legislation will strike a balance between protecting "the privacy rights of individuals while

such information to an institutional third party is reasonably necessary to participate meaningfully in society or in commerce, or is socially beneficial, including to freedom of speech and association; (b) such information is personal, including the extent to which it is intimate and likely to cause embarrassment or stigma if disclosed, and whether outside of the initial transfer to an institutional third party it is typically disclosed only within one's close social network, if at all; (c) such information is accessible to and accessed by non-government persons outside the institutional third party; and (d) existing law, including the law of privilege, restricts or allows access to and dissemination of such information or of comparable information.").

203. *Id.* at 10.

204. *Id.*

205. *Id.*

206. *Id.*

207. Emma Coleman, *One State May Become the First to Ban Law Enforcement Use of Genealogy Databases*, ROUTE FIFTY (Jan. 21, 2020), https://www.routefifty.com/public-safety/2020/01/utah-dna-databases/162544 [https://perma.cc/JJ6J-UG2G].

208. *Id.*

209. *See id.*

giving law enforcement the tools they need to catch the bad guys."[210] He insists the legislation would still allow law enforcement to seek a warrant for a suspect's DNA sample, but would simply prohibit law enforcement from blindly reaching into the databases and hoping for a hit.[211]

CONCLUSION

Identifying dangerous suspects and closing cold cases are of high priority to law enforcement and the communities they serve. The innovative technique of searching public genealogy databases has improved law enforcement's ability to do just that, but it comes at the cost of consumer privacy. Our genetic makeup is the most personal information we have. Unlike a credit card, or even social security number, once it is out in the world, there is no changing it or taking it back. The ever-changing technological landscape of our society is difficult for existing legal doctrine to keep up with, but it is crucial to understand where this new search technique fits in with our expectations of privacy and the Fourth Amendment.

The third-party doctrine says that where an individual voluntarily gives information over to a third party, they lose their expectation of privacy in that information. But the 2018 Supreme Court case, *Carpenter v. United States*, has added to our understanding of the third-party doctrine in light of today's technological changes. Under *Carpenter*, one can argue that the fact that one's genetic information may be in the possession of a third-party should not automatically mean the loss of Fourth Amendment protection—at least where one has a legitimate privacy interest in that information. Yet the act of uploading this information is inarguably a voluntary one, and this may prevent the protection that *Carpenter* might otherwise afford. For this reason, it is crucial that legislatures work to impose clear privacy protections and establish laws ensuring that law enforcement objectives do not erode privacy rights.

210. *Id.*
211. *Id.*