Crime, DNA, and Family: Protecting Genetic Privacy in the World of 23andMe

Victoria Romine*

INTRODUCTION

In 2018, the capture of the "Golden State Killer," also known as the "East Area Rapist" or the "Original Night Stalker," captured the eyes of the nation.[1] The man responsible for at least thirteen murders and fifty rapes—crimes that many thought would never be solved—was taken into custody and charged with capital murder.[2] Why the sudden movement in a case that had been cold for over three decades? Joseph DeAngelo, the now-infamous serial killer, was definitively identified through DNA using a breakthrough new science: genetic genealogy.[3]

At the time, the potential of this new method seemed boundless. The public began to speculate about how many cases could finally be resolved—even infamous cold cases that had haunted communities for decades.[4] The wait was short. Only two months later, John D. Miller was charged with the rape and murder of eight-year-old April Tinsley, who had been kidnapped

---

* J.D. Candidate, 2021; Executive Managing Editor, *Arizona State Law Journal*. Thank you to all the wonderful Editors and Staff Writers on the *Arizona State Law Journal* for their thoughtful editing. Thank you also to my faculty advisor, Professor Jessica Berch, for her guidance, instruction, and encouragement throughout the writing process.

1. Ray Sanchez, Madeline Holcombe & Cheri Mossburg, *Golden State Killer Joseph DeAngelo Sentenced to Life in Prison*, CNN, https://www.cnn.com/2020/08/21/us/golden-state-killer-sentencing/index.html [https://perma.cc/DJ6Z-U9GY] (Aug. 21, 2020, 5:40 PM).

2. *Id.*

3. Emily Shapiro, *The 'Golden State Killer': Inside the Timeline of Crimes*, ABC NEWS (Oct. 30, 2020, 6:39 AM), https://abcnews.go.com/US/inside-timeline-crimes-golden-state-killer/story?id=54744307 [https://perma.cc/Q6XQ-XPPA]. For more information on the Golden State Killer case, see generally MICHELLE MCNAMARA, I'LL BE GONE IN THE DARK (2018). More importantly, to hear from his victims, see ABC10, *Golden State Killer Faces Families of Murder Victims in Court Ahead of His Sentencing*, YOUTUBE (Aug. 20, 2020), https://www.youtube.com/watch?v=hAQk8Czlzoc [https://perma.cc/6LDP-NWAL]; I'LL BE GONE IN THE DARK (HBO television series 2020).

4. *See* Christal Hayes, *Zodiac Killer: Can Genealogy Help Crack the 50-Year-Old Case?*, USA TODAY (May 3, 2018, 9:15 PM), https://www.usatoday.com/story/news/2018/05/03/zodiac-killer-investigators-hope-use-genealogy-site-crack-case/579053002/ [https://perma.cc/VS2Y-ZK7B].

from her Fort Wayne neighborhood in 1988.[5] After the killer repeatedly taunted police, April Tinsley remained one of Indiana's most notorious cold cases before it was solved with genetic genealogy.[6] With the closing of these two major cases, and with many more soon thereafter,[7] both the crimefighting community and the public were convinced that genetic genealogy could be an innovative crime-solving tool that would bring closure to families still waiting for answers to grisly crimes.[8] However, with all of genetic genealogy's promise came questions: questions about privacy, the law—and even its accuracy.[9] This Comment seeks to answer those questions.

Genetic genealogy relies on using data in direct-to-consumer DNA databases to determine familial matches between DNA samples.[10] These

---

5. Eric Levenson & Amanda Watts, *Child-Killer Taunted Investigators for 30 Years with Disturbing Notes. DNA Ends the Mystery of Who Did It, Police Say*, CNN, https://www.cnn.com/2018/07/16/us/cold-case-april-tinsley-dna-trnd/index.html [https://perma.cc/S3TP-B3PF] (July 17, 2018, 6:52 PM). When police questioned Miller at his home prior to his arrest, they asked Miller why he thought they were there. His reply closed a case that had lain dormant for decades: "April Tinsley." *Id.*

6. *Id.*

7. *See* KC Baker, *How Genetic Genealogist CeCe Moore Solved 109 Criminal Cases with DNA: 'It's About Families*,*'* PEOPLE (May 14, 2020, 9:59 AM), https://people.com/crime/how-genetic-genealogist-cece-moore-solved-109-criminal-cases-with-dna-its-about-families/ [https://perma.cc/SV8W-F3UX].

8. *Id.* Genetic genealogy's proponents weren't wrong. Cases nearly sixty years old have been solved using this method. Michael Konopasek, *Officials Announce World's Oldest Cold Case Solved Using Genetic Genealogy in Colorado*, FOX 31 DENVER (Apr. 23, 2020, 9:26 PM), https://kdvr.com/news/local/officials-announce-worlds-oldest-cold-case-solved-using-genetic-genealogy-in-colorado/ [https://perma.cc/28BR-GSSC]. And the Golden State Killer was not the first murderer to be identified using this new method. In 2015, the Phoenix Police Department arrested the infamous "Canal Killer," who had murdered two women along the same canal in the 1990s. Megan Cassidy, *How Forensic Genealogy Led to an Arrest in the Phoenix 'Canal Killer' Case*, AZCENTRAL (Nov. 30, 2016, 6:00 AM), https://www.azcentral.com/story/news/local/phoenix/2016/11/30/how-forensic-genealogy-led-arrest-phoenix-canal-killer-case-bryan-patrick-miller-dna/94565410/ [https://perma.cc/Y9RY-NLQR].

9. Michael Usry was wrongfully accused of rape and murder. Usry became the subject of a murder investigation because of a familial DNA match with his father. Nsikan Akpan, *Genetic Genealogy Can Help Solve Cold Cases. It Can Also Accuse the Wrong Person*, PBS NEWSHOUR (Nov. 7, 2019, 5:15 PM), https://www.pbs.org/newshour/science/genetic-genealogy-can-help-solve-cold-cases-it-can-also-accuse-the-wrong-person [https://perma.cc/6SUK-BCMF]. Although the police eliminated Usry's father due to age, Usry was interrogated and forced to provide a DNA sample—a violation of privacy, as discussed below—to clear his name. *Id.* As it turns out, the original DNA sample linking Usry to the crime was contaminated. *Id.* An unrelated man was later convicted of the crime. Eric Grossarth, *Brian Dripps Pleads Guilty to the Rape and Murder of Angie Dodge*, EAST IDAHO NEWS (Feb. 9, 2021, 11:59 AM), https://www.eastidahonews.com/2021/02/brian-dripps-pleads-guilty-to-the-rape-and-murder-of-angie-dodge/ [https://perma.cc/E8KK-XTKF].

10. Natalie Ram, *Genetic Privacy After* Carpenter, 105 VA. L. REV. 1357, 1376 (2019).

databases, compiled from testing kits available for purchase at any major online retailer,[11] clearly make for an effective crimefighting tool. Although law enforcement has lauded the technology as a groundbreaking innovation for criminal investigation,[12] critics remain concerned with its privacy implications.[13] Not surprisingly, the legal community has joined the discussion. Legal scholars continue to debate whether a person's DNA contains a sufficient privacy interest to be protected by the Fourth Amendment to the Constitution.[14] This debate has grown even more complex as the industry has expanded, and it is further complicated now that the U.S. Supreme Court has decided *Carpenter v. United States*, which was ruled on only two months after Joseph DeAngelo's capture.[15]

Prior to *Carpenter*, the Court had long recognized that a person did not have an expectation of privacy in information held by third parties; therefore, the State did not need a warrant to perform a search.[16] Of course, because consumer DNA testing companies like Ancestry inevitably possess their consumers' DNA samples, the doctrine would have effectively precluded *any* protection for the samples held in these databases. *Carpenter*, in contrast, cast serious doubt on this nearly fifty-year-old doctrine by holding that a person's location information, meticulously archived by her cell phone, was protected by the Fourth Amendment—despite that data being held by a cell-phone

---

11. *Id.*; Steven John, *The Best At-Home DNA Test Kits*, BUS. INSIDER (Feb. 13, 2020, 10:45 AM), https://www.businessinsider.com/best-dna-kit [https://perma.cc/K6LS-MA5S].

12. *See, e.g.*, Press Release, Parabon NanoLabs, Parabon Customers Net 55 Solved Cases in First Year of Snapshot Genetic Genealogy Service (May 8, 2019), https://parabon-nanolabs.com/news-events/2019/05/parabon-customers-net-55-solved-cases-in-first-year-of-snapshot-genetic-genealogy-service.html [https://perma.cc/46HV-7VCR]; Press Release, Florida Dep't of L. Enf't, FDLE Genetic Genealogy Investigations Program Solves Cold Cases in First Year (Oct. 14, 2019), https://www.fdle.state.fl.us/News/2019/October/FDLE-Genetic-Genealogy-Investigations-program-solv [https://perma.cc/R7R9-TU4S].

13. *See, e.g.*, Nila Bala, *Criminal Suspects Deserve Genetic Privacy, Too*, SLATE (Mar. 18, 2019, 7:30 AM), https://slate.com/technology/2019/03/genetic-genealogy-law-enforcement-suspects-dna-privacy-gedmatch.html [https://perma.cc/YH3J-5UQF]; Lindsey Van Ness, *DNA Databases Are Boon to Police but Menace to Privacy, Critics Say*, PEW CHARITABLE TRS.: STATELINE (Feb. 20, 2020), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2020/02/20/dna-databases-are-boon-to-police-but-menace-to-privacy-critics-say [https://perma.cc/8D2Y-RSQT].

14. *See, e.g.*, Ram, *supra* note 10, at 1366–67; George M. Dery III, *Can a Distant Relative Allow the Government Access to Your DNA? The Fourth Amendment Implications of Law Enforcement's Genealogical Search for the Golden State Killer and Other Genetic Genealogy Investigations*, 10 HASTINGS SCI. & TECH. L.J. 103, 107–08 (2019).

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

16. Michael Gentithes, *App Permissions and the Third-Party Doctrine*, 59 WASHBURN L.J. 35, 38–40 (2020); *see also* United States v. Miller, 425 U.S. 435, 442–43 (1976); Smith v. Maryland, 442 U.S. 735, 743–45 (1979).

provider.[17] Now, in a post-*Carpenter* age where almost thirty million people[18] have taken direct-to-consumer ("DTC") DNA tests—and many millions more family members readily identifiable by such tests—it is unclear what, if any, protection the Fourth Amendment provides to a person's DNA.

This Comment proceeds in four parts. Part I provides a brief history of the consumer DNA industry and what privacy risks may be at stake by warrantless law-enforcement access to DTC databases. Part II explains DNA—its function and use by law enforcement—and how the rise of familial DNA testing has worked in conjunction with DTC databases to solve crime. Part III surveys the history of Fourth Amendment jurisprudence and explains why the Court's current standing doctrine limits those who may benefit from the Amendment's protection. And Part IV applies the Court's current Fourth Amendment framework to DNA held by DTC testing companies and argues that because defendants lack standing to bring a Fourth Amendment claim, legislative action is needed to protect the genetic privacy of the millions of people whose information is at risk. Finally, this Comment concludes.

I. THE HISTORY OF DTC TESTING

To fully understand the threat that DTC testing poses to genetic privacy, it is helpful to understand the scope of the issue. This Part provides a brief history of DTC testing before turning to the unintended effects of having such

17. *Carpenter*, 138 S. Ct. at 2217.

18. Kristen Jordan Shamus, *Armed with Massive Data Pools, Genealogy Companies Ancestry, 23andMe Begin COVID-19 Research*, USA TODAY (May 29, 2020, 3:38 PM), https://www.usatoday.com/story/news/health/2020/05/26/genes-dna-ancestry-23-andme-coronavirus-covid-19/5259982002/ [https://perma.cc/J2PY-VK3W] (noting that Ancestry's database contained sixteen million samples); *Frequently Asked Questions—Who Is FamilyTreeDNA?*, FAMILYTREEDNA, https://www.familytreedna.com/ [https://perma.cc/GQR8-RS9J] ("Over 2 million people have tested with FamilyTreeDNA, resulting in the most comprehensive DNA matching database in the industry."); Antonio Regalado, *More than 26 Million People Have Taken an At-Home Ancestry Test*, MIT TECH. REV. (Feb. 11, 2019), https://www.technologyreview.com/2019/02/11/103446/more-than-26-million-people-have-taken-an-at-home-ancestry-test/ [https://perma.cc/NYN5-UEEW] (noting that 23andMe and MyHeritage have tested nine million and two and a half million samples, respectively). Although the most recent data from 2019 put the number of total samples close to 30 million, due to the popularity of the kits in the intervening years, it's likely that the true number is much higher. *See id.*; *DNA Test Kits Market: Increase in Demand for Ancestry Testing To Drive Market*, BIOSPACE (Apr. 27, 2020), https://www.biospace.com/article/dna-test-kits-market-increase-in-demand-for-ancestry-testing-to-drive-market/ [https://perma.cc/FWR6-QBYN]; Press Release, Transparency Mkt. Rsch., DNA Test Kits Market To Exceed Valuation of US$ 2.7 BN by 2030 (Jan. 4, 2021), https://www.transparencymarketresearch.com/pressrelease/dna-test-kits-market.htm [https://perma.cc/7HH8-SF2U].

a large number of DNA samples held by private companies, including the risk of warrantless law-enforcement access.

A. Humble Beginnings

The first major DTC testing database began in 2008 with the launch of 23andMe.[19] For the first time, members of the public could have their DNA tested by professionals and receive a detailed DNA analysis.[20] The analysis provided information about a person's proclivity to more than ninety different traits and propensity to certain health conditions, like Parkinson's disease.[21] Those first 23andMe kits cost about $1,000.[22] The same year, 23andMe was named "Invention of the Year" by *Time*.[23]

Soon thereafter, Ancestry developed its own testing kit.[24] Although 23andMe was principally concerned with providing health and ethnicity information, Ancestry, with its collection of nearly twenty billion historical records, offered an opportunity to use DNA test results to build a person's family tree—and perhaps even connect distant relatives.[25] Ancestry's kit cost

19. Anita Hamilton, *Invention of the Year: 1. The Retail DNA Test*, TIME (Oct. 29, 2008), http://content.time.com/time/specials/packages/article/0,28804,1852747_1854493,00.html [https://perma.cc/5T6D-E8QG]. Although some DNA testing services existed before 23andMe, it was not until that company's launch that the service became widely available to the general public. *See* Anne Belli, *Moneymakers: Bennett Greenspan*, HOUS. CHRON. (July 30, 2011, 10:30 AM), https://www.chron.com/business/article/Moneymakers-Bennett-Greenspan-1657195.php [https://perma.cc/5YTH-58D7] ("The idea for Family Tree DNA . . . launched in early 2000 to provide [a service for those] searching for their ancestors.").

20. Hamilton, *supra* note 19.

21. *Id.*

22. Thomas Goetz, *23AndMe Will Decode Your DNA for $1,000. Welcome to the Age of Genomics*, WIRED (Nov. 17, 2007, 12:00 PM), https://www.wired.com/2007/11/ff-genomics/ [https://perma.cc/ENB3-AF76]; *23andMe History*, 23ANDME, https://mediacenter.23andme.com/assets/timeline/index.html [https://perma.cc/5E54-YXSJ].

23. Hamilton, *supra* note 19.

24. *Our Story*, ANCESTRY CORP., https://www.ancestry.com/corporate/about-ancestry/our-story [https://perma.cc/3C79-GJAR].

25. Brittany Vincent, *At-Home DNA Test Kits: How To Choose the Best Kit for You*, CNN: UNDERSCORED, https://www.cnn.com/2018/09/18/cnn-underscored/dna-kit-guide-shop/index.html [https://perma.cc/5T27-4Z53] (Feb. 11, 2021, 5:11 PM) ("[The AncestryDNA] test is more focused on genealogical history . . . . [23andMe] includes three tests that Ancestry doesn't: genetic health, carrier status and wellness testing."); Press Release, Ancestry Corp., Ancestry Surpasses 15 Million Members in Its DNA Network, Powering Unparalleled Connections and Insights (May 21, 2019), https://www.ancestry.com/corporate/newsroom/press-releases/ancestry-surpasses-15-million-members-its-dna-network-powering-unparalleled [https://perma.cc/Z8YB-VXJR].

only $99.[26] By 2012, 23andMe and Ancestry had begun widely distributing their testing kits for home use, and in doing so, began to develop their own DNA databases.[27]

As 23andMe and Ancestry began to make DTC testing widely available, the founders of GEDmatch were also hard at work. That company was aimed at connecting family members through DNA matches.[28] Although 23andMe and Ancestry could only connect people through the samples in their own respective databases, GEDmatch allowed all DTC customers to upload their test results *regardless of the testing company* and for free.[29] With GEDmatch, consumers were no longer limited to the information held by only Ancestry or only 23andMe and could be matched to their family members no matter which kit they used. GEDmatch thus served as a gap filler, allowing people to connect with relatives who happened to use a different testing company, a status that only grew as various other companies, including FamilyTree DNA[30] and MyHeritage,[31] began infiltrating the market. Thus, it is of little surprise that GEDmatch was the database police used to identify Joseph DeAngelo in 2018.[32]

---

26. Press Release, Ancestry Corp., Ancestry.com Launches New AncestryDNA Service: The Next Generation of DNA Science Poised To Enrich Family History Research (May 3, 2012), https://www.ancestry.com/corporate/newsroom/press-releases/ancestrycom-launches-new-ancestrydna-service-next-generation-dna-science [https://perma.cc/3JDE-6XNV]; Genelle Pugmire, *AncestryDNA Finding Hidden Ancestry*, DAILY HERALD (May 15, 2012), https://www.heraldextra.com/business/technology/ancestrydna-finding-hidden-ancestry/article_a64e7523-14b0-5b92-ae35-62abf44627bc.html [https://perma.cc/44KM-AMBK].

27. Press Release, Ancestry Corp., *supra* note 26; Regalado, *supra* note 18.

28. Jon Schuppe, *New Owner of Consumer DNA Database GEDmatch Vows To Fight Police Search Warrants*, NBC NEWS (Dec. 10, 2019, 4:16 PM), https://www.nbcnews.com/news/us-news/new-owner-consumer-dna-database-gedmatch-vows-fight-police-search-n1099091 [https://perma.cc/PG8L-W88E] ("Rogers . . . founded GEDmatch in Florida nine years ago as a place for people to compare the results of their direct-to-consumer DNA tests in hopes of finding relatives.").

29. *GEDmatch.Com Terms of Service and Privacy Policy*, GEDMATCH, https://www.gedmatch.com/tos.htm [https://perma.cc/275Z-S725] (Dec. 9, 2019); *GEDmatch*, DNA TESTING ADVISER, https://www.dna-testing-adviser.com/GEDmatch.html [https://perma.cc/8KGQ-F9AA].

30. FAMILYTREEDNA, *supra* note 18.

31. MYHERITAGE, https://www.myheritage.com/dna [https://perma.cc/6KRZ-WGCG].

32. Joseph (Joe) Zabel, *The Killer Inside Us: Law, Ethics, and the Forensic Use of Family Genetics*, 24 BERKELEY J. CRIM. L. 47, 50–51 (2019). For a time, GEDmatch also openly allowed law enforcement access to its database, but it later changed its terms of service to provide an "opt-in" provision for anyone who wanted law enforcement to have access to their information. *Id.* at 51 n.20, 52–53; GEDMATCH, *supra* note 29.

B. Unintended Consequences

The purpose of this Section is to provide the scope of the privacy interests at stake with DTC testing. As these kits have gotten less expensive, and as more companies have entered the market, there has been an increase in the number of samples catalogued and a reciprocal risk to privacy. When looking at the current data on this issue, it is important to consider that all of these samples are potentially open to law-enforcement access—and possibly without a warrant.

As of 2020, about thirty million people have taken an at-home DNA test.[33] Although that figure alone might not be cause for concern, it becomes so when one considers that every person taking these tests shares DNA with their genetic relatives.[34] Every person who takes a DTC test has, on average, "nearly 200 third cousins, 950 fourth cousins[,] and 4,700 fifth cousins."[35] Multiply that by thirty million, and the amount of data is staggering. What's more, AncestryDNA purports to provide *over 1,000 years* of ancestral information—meaning that your DNA can be matched with relatives stemming from a relationship literally thousands of years ago.[36] Considering the exponential size of the problem and that GEDmatch offers an opportunity to consolidate all of those samples in one place, the sheer volume of genetic information held by private corporations is astronomical—and it will only continue to grow.

In addition to private databases, police also use publicly funded databases in criminal investigation. The National DNA Index ("NDIS"), the database that collects the DNA of criminal defendants and arrestees, contains nearly twenty million samples.[37] Law enforcement has open access to this system, and states can (and do) require people to surrender their DNA at arrest—without even a criminal charge.[38] This practice has created a database that is expansive and ever-growing as more arrests are made. And as with private databases, each of these samples shares DNA with hundreds, perhaps

---

33. *See* sources cited *supra* note 18.

34. *See infra* Part II.A–B.

35. Akpan, *supra* note 9.

36. *AncestryDNA Test Accuracy*, ANCESTRY, https://www.ancestry.com/lp/genetic-testing/ancestrydna-test-accuracy [https://perma.cc/GM6A-AT9M].

37. *CODIS - NDIS Statistics*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics [https://perma.cc/ZP77-BLET] (noting that the national database contains about fourteen million samples from offenders, four million from arrestees, and one million forensic profiles).

38. *E.g.*, KAN. STAT. ANN. § 21-2511(a) (2021); ARIZ. REV. STAT. ANN. § 13-610(K), (O)(3) (2021); FLA. STAT. § 943.325(7)(b) (2021); *see also* NAT'L CONF. OF STATE LEGISLATURES, DNA ARRESTEE LAWS 4–8 (2013), https://www.ncsl.org/Documents/cj/ArresteeDNALaws.pdf [https://perma.cc/EV9M-4NQ3].

thousands, of others in the population, all potentially free to access without a warrant or a criminal charge.

Needless to say, between the publicly and privately funded databases, law enforcement has access to millions of DNA samples. The question then becomes what, if any, legal protection there may be for those samples. To answer this question, we must first look at DNA itself to understand what information it contains that the Fourth Amendment could possibly embrace. We must also consider how law enforcement uses DNA and whether that use could likewise bring DNA within the scope of the Fourth Amendment.

II. DNA AND LAW ENFORCEMENT

Long before DNA became a staple of criminal investigation, it was known only as an essential component of human biology.[39] DNA is a molecule found inside a cell's nucleus that contains instructions for building proteins, which are read by the body and passed down to offspring during reproduction.[40] While all eukaryotes[41] have DNA, human DNA is unique.[42] Aside from providing uniqueness among individuals, DNA also instructs the body on how to develop as a human, as opposed to a different species.[43] Although knowledge of DNA has been around for centuries,[44] it was not until the 1980s that it began to draw the eye of law enforcement.[45]

---

39. *See* NAT'L LIBR. OF MED., HELP ME UNDERSTAND GENETICS: CELLS AND DNA 6, https://medlineplus.gov/download/genetics/understanding/basics.pdf [https://perma.cc/L5GH-7ZWG]; Nat'l Hum. Genome Rsch. Inst., *Deoxyribonucleic Acid (DNA) Fact Sheet*, GENOME, https://www.genome.gov/about-genomics/fact-sheets/Deoxyribonucleic-Acid-Fact-Sheet [https://perma.cc/5KMR-TXFA] (Aug. 24, 2020).

40. Tim Newman, *What Is DNA and How Does It Work?*, MED. NEWS TODAY (Jan. 11, 2018), https://www.medicalnewstoday.com/articles/319818 [https://perma.cc/XPH2-4UAL].

41. Eukaryotic cells contain DNA in their nuclei and are found in all multi-celled organisms, including humans. *From Prokaryotes to Eukaryotes*, UNDERSTANDING EVOLUTION, https://evolution.berkeley.edu/evolibrary/article/_0/endosymbiosis_03 [https://perma.cc/52YB-AZ8M].

42. *See* Nat'l Hum. Genome Rsch. Inst., *supra* note 39.

43. *Id.*

44. *Id.*

45. *See* Ian Cobain, *Killer Breakthrough—The Day DNA Evidence First Nailed a Murderer*, GUARDIAN (June 7, 2016), https://www.theguardian.com/uk-news/2016/jun/07/killer-dna-evidence-genetic-profiling-criminal-investigation [https://perma.cc/3MNC-FG2P].

A. History of DNA as an Investigative Tool

In the mid-1980s, British geneticist Alec Jeffreys at the University of Leicester discovered that DNA could be used for human identification.[46] Recognizing the importance of the discovery, Jeffreys began giving lectures on how DNA could be used to solve crime.[47] Shortly thereafter, law enforcement in Narborough contacted Jeffreys about using DNA to solve the murder of two young women, whom the police suspected were victims of the same killer.[48] DNA soon exonerated the lead suspect,[49] and after an extensive collection of voluntary DNA samples, police arrested the true culprit.[50]

From there, the use of DNA in criminal investigations blossomed into the gold standard of forensic reliability.[51] It soon became standard practice for law enforcement to catalogue DNA samples from convicted felons into statewide databases.[52] Then, in 1994, the FBI implemented the Combined DNA Index System ("CODIS") software, which allowed police to search DNA samples in both state and national databases.[53] Since then, states have enacted various DNA-collection procedures, with some states allowing DNA collection when a person is booked into jail (pretrial and perhaps pre-charge) and others cataloging after conviction.[54]

---

46. Ron Yaxley, *DNA Fingerprinting*, 15 COMMONWEALTH L. BULL. 614, 614 (1989).

47. Cobain, *supra* note 45.

48. *Id.*

49. Yaxley, *supra* note 46, at 618. In the years since, DNA has been used to exonerate thousands of people who have been wrongfully convicted. For more information on how DNA can be used to exonerate instead of incarcerate, see Simon A. Cole, *Forensic Science and Wrongful Convictions: From Exposer to Contributor to Corrector*, 46 NEW ENG. L. REV. 711 (2012).

50. Yaxley, *supra* note 46, at 618–19.

51. Erin Murphy, *The Art in the Science of DNA: A Layperson's Guide to the Subjectivity Inherent in Forensic DNA Typing*, 58 EMORY L.J. 489, 490 (2008) ("DNA typing is typically held out as the pinnacle of 'good' forensic evidence, in that it exemplifies the kind of scientific rigor that first-generation techniques lack."); *How DNA Analysis Has Revolutionised Criminal Justice*, DEAKIN UNIV.: THIS., https://this.deakin.edu.au/career/how-dna-analysis-has-revolutionised-criminal-justice [https://perma.cc/H2SH-6URS].

52. *See* Karen Cormier et al., *Evolution of DNA Evidence for Crime Solving—A Judicial and Legislative History*, FORENSIC MAG., June–July 2005, at 1.

53 Jay Miller, *Combined DNA Index System (CODIS)*, 44 U.S. ATT'YS BULL. 154, 154–55 (1996); *Combined DNA Index System*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis [https://perma.cc/AR94-HVZ2].

54. *Compare, e.g.*, KAN. STAT. ANN. § 21-2511(a) (2021) (DNA collected at arrest), *and* ARIZ. REV. STAT. ANN. § 13-610(K), (O)(3) (2021), *with* MINN. STAT. § 609.177(1) (2021) (DNA collected upon sentencing), *and* IOWA CODE § 81.2(1) (2021); *Where States Stand on DNA Collection*, PROPUBLICA (May 5, 2009, 7:40 AM), https://www.propublica.org/article/where-states-stand-on-dna-collection-505 [https://perma.cc/Y3MX-RGG5].

CODIS has revolutionized criminal investigation.[55] Since its inception, CODIS has solved countless crimes using Short Tandem Repeats ("STRs") to produce matches between two or more samples of DNA.[56] STRs are areas of a person's DNA that are repeated.[57] Commonly called "stutters," these repeats vary among individuals and allow CODIS to produce a "match" when two samples share STRs.[58] Although comparing STRs between DNA samples can identify a match, the STRs themselves reveal no other information.[59] The only information law enforcement receives is that one sample matches another: that one person produced both samples.[60] After receiving a match in CODIS, prosecutors can use the information to seek a conviction.[61] Over the years, this practice has been used extensively, and police have even used DNA to solve cold cases decades after a crime is committed, with some identifications occurring over half a century later.[62] Moreover, since DNA lasts after death, police can exhume a person's body to test his DNA against a sample at a crime scene.[63] In recent years, however, DNA technology has developed even further.

---

55. Michelle Hibbert, *DNA Databanks: Law Enforcement's Greatest Surveillance Tool?*, 34 WAKE FOREST L. REV. 767, 768 (1999).

56. *Frequently Asked Questions on CODIS and NDIS*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet [https://perma.cc/4BVF-7F6F].

57. Murphy, *supra* note 51, at 495; Greg Miller, *Familial DNA Testing Scores a Win in Serial Killer Case*, SCI. MAG., July 16, 2010, at 262.

58. Miller, *supra* note 57; *see also* FED. BUREAU OF INVESTIGATION, *supra* note 53.

59. *See* Ram, *supra* note 10, at 1377–78.

60. *Id.*

61. *See* Cormier et al., *supra* note 52.

62. *See, e.g.*, Travis Fedschun, *Cold Case Killing of Woman, 80, Cracked After 30 Years by DNA Test, 'Perseverance' by Detectives*, FOX NEWS (May 8, 2019), https://www.foxnews.com/us/cold-case-killing-south-carolina-dna-detective-work-georgia [https://perma.cc/CS88-2H5K] (thirty years); Trevor J. Mitchell, *Rapid City Police Solve 51-Year-Old Cold Case with Help of Genealogy*, ARGUS LEADER (June 17, 2019, 6:48 PM), https://www.argusleader.com/story/news/2019/06/17/rapid-city-police-solve-51-year-old-cold-case-genealogy-gwen-miller/1481518001/ [https://perma.cc/U5LA-87V7] (fifty-one years); N'dea Yancey-Bragg, *DNA from an Old Razor Helped Police Solve 41-Year-Old Rape and Murder Cold Case*, USA TODAY (May 15, 2019, 3:09 PM), https://www.usatoday.com/story/news/nation/2019/04/18/old-razor-41-year-old-california-cold-case/3515419002/ [https://perma.cc/VYD5-E9TC] (forty-one years).

63. *See* Dan Bloom, *Could One of America's Oldest Missing Person Cases Finally Be Solved? Investigators Hope DNA Will Unravel Mystery of Man Who Vanished in 1926*, DAILY MAIL (Apr. 30, 2014, 11:20 AM), https://www.dailymail.co.uk/news/article-2616542/DNA-sought-close-1926-missing-person-case.html [https://perma.cc/K8JY-HH5Z] (reporting that the DNA of a skeleton that was over 160 years old could be used to solve a missing person case from 1926).

B. Familial DNA

Familial DNA testing has recently emerged as a different way to use CODIS and STR testing to solve crime. This type of DNA testing focuses on two considerations: (1) specific regions in a person's chromosomes and (2) how those regions compare to the general population.[64] The regions examined contain STRs.[65] While the repetitions vary among individuals, family members generally share them.[66] If a person shares STRs with someone else, there is a likelihood that the two individuals are related.[67] The second prong of the analysis determines how common those repetitions are in the general population.[68] Shared repetitions that are not common among the general population indicate a likely familial relationship.[69]

With familial DNA testing, law enforcement can use CODIS to look for shared areas of STRs in DNA samples, producing familial matches.[70] Once CODIS completes the STR analysis, it produces a ranked list of individuals likely to be related to the sample in question.[71] This list can then be used to narrow law enforcement's search, potentially leading to a suspect and ultimate conviction.[72]

Familial DNA testing has been around since 2008, when California became the first state to implement the practice.[73] It has seen wavering support since, with critics concerned with Fourth Amendment issues and the impact on racial minorities: there are more samples from Black people in the national database than samples from white individuals.[74] In contrast, familial DNA testing has seen immense success in solving cold cases, including the

64. Miller, *supra* note 57.
65. *Id.*
66. *Id.*
67. *Id.*
68. *Id.*
69. *Id.*
70. *Id.*
71. *Id.*
72. *See id.*
73. Eli Rosenberg, *Family DNA Searches Seen as Crime-Solving Tool, and Intrusion on Rights*, N.Y. TIMES (Jan. 27, 2017), https://www.nytimes.com/2017/01/27/nyregion/familial-dna-searching-karina-vetrano.html [https://perma.cc/98EG-C323]; MICHAEL B. FIELD ET AL., STUDY OF FAMILIAL DNA SEARCHING POLICIES AND PRACTICES 14 (2017), https://www.ncjrs.gov/pdffiles1/nij/grants/251081.pdf [https://perma.cc/76NK-J8L4].
74. Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291, 336–37 (2010); Sonia M. Suter, *All in the Family: Privacy and DNA Familial Searching*, 23 HARV. J.L. & TECH. 309, 370 (2010) ("The fact that minority groups are over-represented in DNA databases necessarily means that the pool of individuals subject to future searches for matching DNA profiles in criminal investigations will disproportionately include minorities.").

notorious "Grim Sleeper" serial killer of California.[75] Despite the privacy and racial concerns surrounding familial DNA testing, twelve of the most populous—and racially diverse—states currently allow it.[76] Only one state, Maryland, has forbidden the practice altogether.[77] Notably, however, in the states where familial DNA testing is legal, nearly all impose limits on when it can be used: most frequently in cases involving public safety risks, violent crimes, or after the exhaustion of all other investigatory leads.[78]

Genetic genealogy involves a similar type of familial DNA testing to that used in public databases.[79] However, the amount of information revealed by familial testing in DTC databases differs greatly from that found in public databases. Although CODIS focuses on STRs, DTC databases analyze

---

75. 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 [https://perma.cc/N7UU-Y8E2]; Suzanne Zuppello, *'Grim Sleeper' Serial Killer: Everything You Need To Know*, ROLLING STONE (Aug. 18, 2016, 5:59 PM), https://www.rollingstone.com/culture/culture-features/grim-sleeper-serial-killer-everything-you-need-to-know-252246/ [https://perma.cc/84HD-N2VX]. Arizona has seen its own success with familial DNA; the method was used to solve the murder of Allison Feldman in Scottsdale, Arizona, in 2018. Her killer had been in police custody three separate times after the murder, but police never suspected him of the crime until they received a familial DNA match. Uriel J. Garcia, *How Familial DNA Search Was Used To Find Scottsdale Murder Suspect in Allison Feldman Case*, AZCENTRAL (Apr. 16, 2018, 4:14 PM), https://www.azcentral.com/story/news/local/scottsdale/2018/04/16/how-familial-dna-search-used-find-scottsdale-murder-suspect-ian-mitcham-allison-feldman/509143002/ [https://perma.cc/88N7-NVYJ].

76. These include Arizona, California, Colorado, Florida, Minnesota, New York, Ohio, Texas, Utah, Virginia, Wisconsin, and Wyoming. Rainey, *supra* note 75; *Most Diverse States 2021*, WORLD POPULATION REV., https://worldpopulationreview.com/state-rankings/most-diverse-states [https://perma.cc/YFK2-QAQC].

77. Rainey, *supra* note 75; *see also* MD. CODE ANN., PUB. SAFETY § 2-506(d) (West 2021).

78. *See, e.g.*, CAL. OFF. OF THE ATT'Y GEN., MEMORANDUM OF UNDERSTANDING: DOJ FAMILIAL SEARCHING PROTOCOL 1–2, https://oag.ca.gov/sites/all/files/agweb/pdfs/bfs/fsc-mou-06072019.pdf? [https://perma.cc/JS9Z-4KHW]; ARIZ. DEPT. OF PUB. SAFETY SCI. ANALYSIS BUREAU, FAMILIAL DNA ANALYSIS 1 (2019), http://www.azdps.gov/sites/default/files/media/Familial%20DNA%20Analysis%20Flyer_0.pdf [https://perma.cc/Q3U9-3SQR]; Allison Murray et al., *Familial DNA Testing: Current Practices and Recommendations for Implementation*, INVESTIGATIVE SCIS. J., Sept. 2017, at 1, 5 ("With few exceptions, all states who currently conduct familial DNA searching only perform these searches on unsolved serious violent crimes where all investigative efforts have been exhausted."); CAROLINE O. MOORMAN, THE USE OF FAMILIAL DNA SEARCHES: A POLICY ANALYSIS 15–20 (2012), https://epublications.regis.edu/cgi/viewcontent.cgi?article=1255&context=theses [https://perma.cc/U6PC-67R2]. *See generally* FIELD ET AL., *supra* note 73 (explaining the requirements in Colorado, California, and Wisconsin for law enforcement to request familial DNA testing).

79. Akpan, *supra* note 9; *Snapshot Genetic Genealogy*, PARABON NANOLABS, https://snapshot.parabon-nanolabs.com/genealogy [https://perma.cc/97A9-TTDA].

single-nucleotide polymorphisms ("SNPs").[80] STRs generally provide only matches or partial matches between DNA samples, but SNPs reveal information about a person's sex, physical appearance, medical conditions, genetic history, and ancestral origin.[81] This information allows law enforcement to create extensive family trees, developing a whole family of potential suspects to investigate.[82] Despite the differences between these databases and CODIS, however, there are currently no procedural protections regulating what law enforcement can do with publicly available DNA databases outside of private user agreements.[83] Currently, none of the available DTC databases allow a user's genetic relatives to "opt out" of law-enforcement access, despite the personal information retained.[84] Moreover, some databases, like GEDmatch and FamilyTreeDNA, explicitly *allow* law enforcement access in some circumstances.[85] Therefore, if DNA is to be protected, such protection must come from the law.

---

80. Ram, *supra* note 10, at 1382 n.141; Zabel, *supra* note 32, at 57–58.

81. Zabel, *supra* note 32, at 57. There is even evidence that DNA can help estimate the length of a person's life. *See* James Randerson, *What DNA Can Tell Us*, GUARDIAN (Apr. 26, 2008, 7:01 PM), https://www.theguardian.com/science/2008/apr/27/genetics.cancer [https://perma.cc/EPD2-JQA9]; *see also* George D. Dalton et al., *New Insights into the Mechanism of Action of Soluble Klotho*, FRONTIERS IN ENDOCRINOLOGY (Nov. 17, 2017), https://www.frontiersin.org/articles/10.3389/fendo.2017.00323/full [https://perma.cc/RZ2R-S8AW] ("[T]ransgenic mice that overexpress *klotho* exhibit an extended lifespan compared with [other mice].").

82. Akpan, *supra* note 9; PARABON NANOLABS, *supra* note 79.

83. Kristen V. Brown, *No One Is Safeguarding Your DNA*, BLOOMBERG BUSINESSWEEK (Feb. 26, 2019, 4:00 AM), https://www.bloomberg.com/news/articles/2019-02-26/law-enforcement-can-do-whatever-it-likes-with-consumer-dna-data [https://perma.cc/H68A-V5GN]; Ram, *supra* note 10, at 1361–65; Claire Abrahamson, Note, *Guilt by Genetic Association: The Fourth Amendment and the Search of Private Genetic Databases by Law Enforcement*, 87 FORDHAM L. REV. 2539, 2251–53 (2019).

84. Most DNA testing companies require a court order to turn over information contained in their databases. *See, e.g.*, *23andMe Guide for Law Enforcement*, 23ANDME, https://www.23andme.com/law-enforcement-guide/ [https://perma.cc/AX92-3CZ5]; *Ancestry Guide for Law Enforcement*, ANCESTRY, https://www.ancestry.com/cs/legal/lawenforcement [https://perma.cc/E342-2SJ8]. However, this limitation does little to protect the information of consumers' genetic relatives, and open-source databases like GEDmatch, which collect data from companies with more stringent requirements, are searchable by anyone with an account. Bala, *supra* note 13.

85. *Law Enforcement Matching—Frequently Asked Questions*, FAMILYTREEDNA, https://learn.familytreedna.com/ftdna/law-enforcement-faq/ [https://perma.cc/EWZ6-TJ2U]; GEDMATCH, *supra* note 29.

III. THE FOURTH AMENDMENT FRAMEWORK

The Fourth Amendment serves as a cornerstone of the constitutional protection of individual privacy. It guarantees that

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[86]

The Supreme Court has interpreted the Fourth Amendment to mean that when a government agent, usually law enforcement, conducts a "search" or "seizure," the act must be "reasonable," either because a warrant supported by probable cause has been issued or because the circumstances otherwise make the search or seizure reasonable.[87] Moreover, the Fourth Amendment standing doctrine limits *who* can bring a Fourth Amendment claim.[88] If a defendant can show that he has standing and that police conducted an unreasonable search or seizure, a court can exclude the evidence found during the search and any "fruit of the poisonous tree"—evidence found as a direct result of the search.[89]

A. Searches

The first query in a Fourth Amendment analysis is whether a search has occurred. Although the search requirement has traditionally been construed as protecting property, the Supreme Court in *Katz v. United States* held that "the Fourth Amendment protects people, not places."[90] That statement marked a shift away from the focus on property and began the Court's transition to protecting individual privacy under the Fourth Amendment.[91] In the years since, the Court has applied a two-prong privacy test to determine whether police action constitutes a search subject to Fourth Amendment protection: (1) a person must "exhibit[ ] an actual (subjective) expectation of privacy," and (2) the expectation must be "one that society is prepared to

86. U.S. CONST. amend. IV.

87. *See* Carpenter v. United States, 138 S. Ct. 2206, 2213–14 (2018); Maryland v. King, 569 U.S. 435, 447–48 (2013).

88. Rakas v. Illinois, 439 U.S. 128, 136–40 (1978).

89. Wong Sun v. United States, 371 U.S. 471, 484–88 (1963); *see* Mapp v. Ohio, 367 U.S. 643, 658 (1961).

90. 389 U.S. 347, 351, 358–59 (1967).

91. That being said, the Court has revived the property approach in recent years. *See, e.g.*, United States v. Jones, 565 U.S. 400, 405–07 (2012). However, that approach is outside the scope of this Comment.

recognize as 'reasonable.'"[92] Focusing on privacy instead of property, the Court in *Katz* found that the placing of a police wiretap on the outside of a phone booth was a search protected by the Fourth Amendment.[93]

Although *Katz* refocused the Fourth Amendment onto privacy interests, the Supreme Court also developed the third-party doctrine, which limits the definition of reasonable privacy interests. The third-party doctrine posits that a person does not have a reasonable expectation of privacy in what he shares with others.[94] In *United States v. Miller*, the Court held that bank records showing the defendant's financial transactions were not protected under the Fourth Amendment.[95] The Court noted that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[96] Because the defendant knew the bank had access to his financial information, he had no reasonable expectation of privacy and thus no protection.[97]

The Court found similarly in *Smith v. Maryland*. In that case, the Court held that the use of a pen register to determine who was calling a robbery victim was not protected by the Fourth Amendment.[98] The Court again emphasized that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[99] Because the defendant's identity and the numbers he dialed were transmitted to the phone company when he placed the call, the information was voluntarily given, so the defendant did not have a reasonable expectation of privacy in the information.[100]

B. Reasonableness

Even if a search has occurred under the Fourth Amendment, that alone is not enough for the suppression of evidence.[101] The defendant must also show that the search was unreasonable.[102] The general rule is that a warrant supported by probable cause will make most searches reasonable.[103] In the absence of a warrant, the government must show that the circumstances of

92. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
93. *Id.* at 358–59 (majority opinion).
94. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 442–43 (1976).
95. *Miller*, 425 U.S. at 444–45.
96. *Id.* at 442 (alteration in original) (quoting *Katz*, 389 U.S. at 351).
97. *Id.* at 442–43.
98. *Smith*, 442 U.S. at 744–46.
99. *Id.* at 743–44.
100. *Id.* at 745–46.
101. Maryland v. King, 569 U.S. 435, 446–47 (2013).
102. *Id.* at 447.
103. *See* Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

the search justify an exception.[104] To meet that standard, law enforcement must establish a legitimate interest outside of criminal investigation that outweighs the individual's privacy interest.[105] Generally, this inquiry considers the scope and degree of the intrusion on privacy and the importance of the government interest at issue.[106] For example, the Court has found such justifying circumstances when law enforcement acts to provide emergency aid to an injured person or to search a suspect for weapons after an arrest.[107] If there is no warrant, and a court finds that the circumstances do not justify an exception, a search will be deemed unreasonable.[108]

C. Standing

Even if a Fourth Amendment violation has occurred—that is, law enforcement has performed an unreasonable search—the unlawful search alone is not enough for suppression of evidence. To succeed on a motion to suppress, the defendant must also have standing.[109] The Fourth Amendment standing doctrine requires the person seeking suppression (the defendant) to be the person whose rights were invaded.[110] The crux of this issue is whether the defendant has a reasonable expectation of privacy in the items or locations searched.[111] If the answer is no, then the defendant cannot have the evidence excluded at trial.[112] A standing issue usually arises when someone other than the defendant has been searched.[113] If another person has a reasonable expectation of privacy in the items or locations searched, and the police do not have a warrant and no exception applies, the search violates the Fourth Amendment.[114] However, because that violation occurred against the other person—not *against the defendant*—evidence from the search may be used against the defendant at trial.[115] Thus, in a Fourth Amendment claim for

104. *Id.* at 2221–23.

105. *King*, 569 U.S. at 448.

106. *Id.* at 448–49; *see also* Schmerber v. California, 384 U.S. 757, 767–69 (1966).

107. Kentucky v. King, 563 U.S. 452, 460 (2011); Chimel v. California, 395 U.S. 752, 762–63 (1969).

108. *Carpenter*, 138 S. Ct. at 2221; *King*, 569 U.S. at 447–48.

109. *See* Rakas v. Illinois, 439 U.S. 128, 132 (1978).

110. *Id.* at 134.

111. *Id.* at 143.

112. *See id.* at 148–49.

113. *See, e.g.*, United States v. Payner, 447 U.S. 727, 730–31 (1980) (holding that the defendant did not have standing to challenge the search of a third party's briefcase); *Rakas*, 439 U.S. at 130, 148 (holding that the defendants did not have standing to challenge the search of another person's car).

114. *See* U.S. CONST. amend. IV; Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

115. *See Rakas*, 439 U.S. at 133.

suppression, courts must consider whether the defendant himself has been the victim of an unconstitutional search.[116]

IV. THE FOURTH AMENDMENT AND PRIVACY: *CARPENTER* AND *KING*

Although the Fourth Amendment protects privacy, the Supreme Court has been slow—if not reluctant—to adapt its definition of "privacy" to the twenty-first century.[117] This Part explores the Court's reasoning in *Maryland v. King*, where the Court held that law enforcement can take and store a person's DNA during jail booking procedures, which take place before any trial or conviction. It also examines recent shifts in the doctrine that have indicated more of a willingness to bring the Amendment closer to modern views of privacy. That was the focus of *Carpenter v. United States*, which is explored in Section B. Both cases illustrate the current state of Fourth Amendment jurisprudence and provide a useful backdrop for how a court would analyze a claim for suppression based on evidence obtained through the search of a DTC database.

A. DNA and Reasonableness: Maryland v. King

In *King*, the Court upheld a Maryland statute that required police to collect a person's DNA upon being booked into jail.[118] Alonzo Jay King, Jr. was arrested for assault, and police collected his DNA pursuant to the statute.[119] After running King's DNA through the national law-enforcement database, police were alerted to a DNA match between King and an unsolved rape case.[120] King was subsequently convicted of the rape.[121]

Despite the Court conceding that the police's intrusion into King's body via a buccal swab was a search, it found that "some circumstances, such as '[w]hen faced with special law enforcement needs, diminished expectations

116. *See Payner*, 447 U.S. at 731.

117. *See* Amelia Thomson-DeVeaux, *The Supreme Court Is Stubbornly Analog—By Design*, FIVETHIRTYEIGHT (May 29, 2018, 9:00 AM), https://fivethirtyeight.com/features/the-supreme-court-is-stubbornly-analog-by-design/ [https://perma.cc/9GFM-3XBY]; David Grossman, *5 Times the Supreme Court Changed the Future of Technology*, POPULAR MECHS. (Dec. 30, 2016), https://www.popularmechanics.com/technology/g2881/supreme-court-changed-tech/ [https://perma.cc/QT5Z-5RVD]; *see also* Mark Sherman & Jessica Gresko, *You've Reached the Supreme Court. Press 1 for Live Arguments*, ASSOCIATED PRESS (Apr. 22, 2020), https://apnews.com/article/19b82f029dcb760dc7f0c644472192fb [https://perma.cc/6C32-VPXS].

118. Maryland v. King, 569 U.S. 435, 465–66 (2013).

119. *Id.* at 441.

120. *Id.*

121. *Id.*

of privacy, minimal intrusions, or the like . . . may render a warrantless search or seizure reasonable.'"[122] To evaluate whether such circumstances existed, the Court balanced law enforcement's interest in identification and safety with the defendant's right to privacy.[123]

The Court found that King underwent a reasonable search based on a "minimal" intrusion into his privacy interest.[124] The Court noted that the physical intrusion into King's body "involve[d] but a light touch on the inside of the cheek" and "require[d] no 'surgical intrusions beneath the skin.'"[125] The *King* Court also considered the plethora of procedural protections under the Maryland statute, including that the testing was limited because "information in the [national] database is only useful for human identity testing."[126] The Court left open the question whether purposes other than identity would bring the practice into the protection of the Fourth Amendment, stating "[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."[127] Because the police action was "minimally invasive" and revealed little personal information, King's privacy interest, although present, was diminished.[128]

In contrast, the Court found a substantial government interest in the identification of arrestees.[129] The Court emphasized that proper identification was imperative for arraignment—in which it is necessary to present the proper person—and also for determining an arrestee's background and whether he posed a safety risk to police officers and jailhouse staff.[130] Although the Court conceded that "[w]hen the police stop a motorist at a checkpoint . . . the Court has insisted on some purpose other than 'to detect evidence of ordinary criminal wrongdoing' to justify . . . searches in the absence of individualized suspicion," it found that the law-enforcement interest in identification for safety purposes outweighed King's diminished expectation of privacy.[131]

---

122. *Id.* at 446–47 (quoting Illinois v. McArthur, 531 U.S. 326, 330 (2001)).

123. *See id.* at 448–49, 465.

124. *Id.* at 461.

125. *Id.* at 446 (quoting Winston v. Lee, 470 U.S. 753, 760 (1985)).

126. *Id.* at 445 (quoting JOHN M. BUTLER, FUNDAMENTALS OF FORENSIC DNA TYPING 279 (2009)).

127. *Id.* at 464–65.

128. *See id.* at 460, 465.

129. *Id.* at 460–61.

130. *Id.* at 450–53.

131. *Id.* at 462–63 (quoting City of Indianapolis v. Edmond, 531 U.S. 32, 38 (2000)).

Justice Scalia dissented, expressing deep concerns that law enforcement's motive was *precisely* "to detect evidence of ordinary criminal wrongdoing" because the results of the DNA test were not released until *after* arraignment and certainly after any safety risk would have arisen in the jail.[132] The purposes provided by the Court (identification and safety), therefore, could not possibly have been the true motivations for the collection of King's DNA.[133] Despite this concern, the majority held that the Maryland statute did not violate the Fourth Amendment.[134]

B. A Modernized Third-Party Doctrine: Carpenter v. United States

Although in *King* the Supreme Court seemed less willing to protect individual privacy, the Court took the opposite position in *Carpenter*. Despite the precedents in *Smith* and *Miller* that established a seemingly boundless third-party doctrine, the Court narrowed its scope in *Carpenter*.[135] In *Carpenter*, the defendants were charged with robbing several electronics stores over a period of months.[136] Law enforcement received court orders under the Stored Communications Act to obtain the cell phone records of the defendants, including their cell-site location information ("CSLI"), which tracks a person's GPS location via her cell phone.[137] Because the Stored Communications Act requires a lower standard than probable cause, the defendants challenged the constitutionality of the court orders, arguing that the government had violated their Fourth Amendment rights.[138]

The main issue in *Carpenter* was whether a person has a reasonable expectation of privacy in her CSLI, despite it being held by cell-phone providers—or third parties.[139] If, as was the traditional understanding, a person truly has no expectation of privacy in information possessed by third parties, the defendants would have had no claim. However, instead of relying on the precedents in *Smith* and *Miller* to decide the case, the Court evaluated whether the policy considerations behind the third-party doctrine were actually advanced by allowing law enforcement to have warrantless access to CSLI.[140] In this analysis, the Court considered the time period in question, the

132. *Id.* at 468–72 (Scalia, J., dissenting).
133. *Id.* at 469–73.
134. *Id.* at 465–66 (majority opinion).
135. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).
136. *Id.* at 2212.
137. *Id.*
138. *Id.* at 2212, 2221. Warrants require probable cause. U.S. CONST. amend. IV ("[N]o Warrants shall issue, but upon probable cause . . . .").
139. *Carpenter*, 138 S. Ct. at 2217–20.
140. *Id.* at 2219–20.

pervasiveness of the device, and what other information outside of physical movements could be revealed by the data.[141] The Court also questioned whether the defendant "voluntarily" shares his information with third parties when he takes no affirmative act to do so, thus calling into question whether the third-party doctrine as expounded in *Smith* and *Miller* was implicated at all.[142] Ultimately, the Court decided that CSLI was of an "intimate" enough nature to justify an exception to the third-party doctrine, and thus law enforcement needed a warrant to access it.[143]

Time was an essential consideration in *Carpenter*.[144] The Court noted that "[m]apping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts" and expressed concern that a person's physical movements could be recorded for five years, which is how long cell carriers store the information.[145] Unlike past technologies, where "attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection," CSLI had no such limitations and thus posed a unique privacy concern.[146] This weighed in favor of finding CSLI protected by the Fourth Amendment.[147]

The Court also considered the pervasiveness of cell phones in modern society.[148] The Court noted that "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."[149] Likening a cell phone to a "feature of human anatomy," the Court concluded that because people carry their cell phones to private locations, there is an expectation of privacy.[150] The Court explained that there was even more of an expectation of privacy in a cell phone than an automobile, which it had recently found unprotected, because "[w]hile individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner."[151] Thus, the Court considered modern notions of privacy in determining that there was a reasonable expectation of privacy in CSLI.[152]

---

141. *See id.* at 2217, 2220.
142. *Id.* at 2219–20.
143. *Id.* at 2220.
144. *Id.* at 2217–18.
145. *Id.*
146. *Id.* at 2218.
147. *Id.*
148. *Id.* at 2220.
149. *Id.* (quoting Riley v. California, 573 U.S. 373, 385 (2014)).
150. *Id.* at 2218.
151. *Id.*
152. *Id.* at 2220.

The Court further noted that CSLI reveals more than just location information.[153] It found that CSLI has the power to reveal a person's "familial, political, professional, religious, and sexual associations."[154] Specifically, the Court was concerned with CSLI's ability to go "beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales."[155] Because CSLI could reveal private information, it implicated privacy interests—despite being held by third parties.[156]

Finally, in evaluating the policy behind the third-party doctrine, the Court questioned whether the third-party doctrine could even be applied absent an affirmative, voluntary act. The Court quoted *Smith* and reiterated that "a person has no legitimate expectation of privacy in information he *voluntarily* turns over to third parties."[157] The Court distinguished *Smith*, however, noting that a plethora of activities, including "incoming calls, texts, or e-mails," could generate CSLI despite not being initiated by the user, which was the case in *Smith*.[158] The *Carpenter* Court thus focused on the voluntariness requirement and questioned whether sharing CSLI was accomplished through an affirmative act of consent.[159] The Court noted that "[a]part from disconnecting the phone from the network, there [was] no way to avoid leaving behind a trail of location data."[160] Therefore, absent consent—or at least the ability to "disconnect[ ]" from the collection of data—the defendants did not give up their right to privacy just because the cell phone companies automatically recorded the data.[161]

After carefully weighing the above factors and considering whether the third-party doctrine should even apply to involuntary acts, the Court concluded that the defendants had a reasonable expectation of privacy in their CSLI, and that privacy interest was not diminished by the cell-phone companies' collection of that data.[162] Consequently, a search had occurred within the context of the Fourth Amendment, satisfying that element of a

153. *Id.* at 2217.

154. *Id.* (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

155. *Id.* at 2218.

156. *Id.* at 2217–18.

157. *Id.* at 2216 (emphasis added) (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).

158. *See Carpenter*, 138 S. Ct. at 2220; *Smith*, 442 U.S. at 744.

159. *Carpenter*, 138 S. Ct. at 2220.

160. *Id.*

161. *Id.*

162. *See id.* at 2221–23. The Court maintained that a sufficient government interest would still justify the search and make it reasonable, if those circumstances were present. *Id.* at 2222–23.

suppression claim.[163] The Court then determined that the search was unreasonable because "cases establish that warrantless searches are typically unreasonable where 'a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing.'"[164] Because the CSLI was sought without a warrant and as evidence in a criminal investigation—not for other, non-investigatory reasons like safety—the Fourth Amendment protected it from law enforcement.[165]

V. THE FOURTH AMENDMENT AND DTC DATABASES

Based on *Carpenter* and *King*, the Fourth Amendment likely protects a person's DNA. However, defendants will rarely have standing to protect that privacy interest, despite the protections the Court was willing to extend in *Carpenter*. This gap between the law and traditional notions of privacy must be closed in order to secure the privacy of both defendants and the users of DTC databases.

A. Familial Searching of DTC Databases Is a Search

With *Carpenter*'s increased focus on consent, it is likely that even under more stringent applications of the third-party doctrine like those found in *Smith* and *Miller*, a court would find that the third-party doctrine does not apply to consumer DNA samples because a defendant does not voluntarily act to share his DNA with DTC databases like Ancestry. However, even if a court finds that a person does act voluntarily and must evaluate whether *Carpenter*'s exception based on the "intimate" nature of the information should apply, a person's DNA will likely meet the *Carpenter* standard. Therefore, because a person has a reasonable expectation of privacy in his DNA, law enforcement's use of DTC databases constitutes a search under the Fourth Amendment, despite any obstacle from the third-party doctrine.

1. The Third-Party Doctrine Does Not Apply to DNA Given Involuntarily

The government's best argument that warrantless access to DTC databases is not a search is the third-party doctrine. Because the DNA is held by private companies (third parties), the third-party doctrine might preclude any

163. *Id.* at 2220.
164. *Id.* at 2221 (quoting Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 652–53 (1995)).
165. *Id.* at 2221–23.

protection. However, it is likely that the third-party doctrine no longer applies under these circumstances. In *Carpenter*, the Court considered the voluntariness of sharing CSLI data with cell-phone companies. Even before that, *Smith* emphasized the need for a voluntary act in third-party doctrine cases, and *Miller* required the defendant to "knowingly" convey the information. Thus, the third-party doctrine only applies when the defendant willfully makes the choice to share his information—or, at least, when he knows it is shared and does not withdraw consent.[166]

Notably, none of the prevalent DNA testing companies require consent from a consumer's genetic relatives to retain the consumer's DNA.[167] The inherent problem with this practice is that individuals' private information is turned over to testing companies without any consent from the individuals themselves. This raises a "voluntariness" issue because although the consumer may make an affirmative act, the genetic relatives never do. The *Carpenter* Court noted that a person does not make any affirmative act when receiving incoming calls and messages—these are acts made by others. Thus, like in *Carpenter*, a court should find the defendant makes no affirmative act when his relative exposes his genetic information to the public—and to law enforcement.

2. If the Third-Party Doctrine Applies to Familial DNA Searching, the DNA in Consumer Databases Falls Within the *Carpenter* Exception

Despite the absence of the defendant's affirmative act, even if a court does apply the third-party doctrine to DNA in DTC databases, it should fall within *Carpenter*'s exception for "intimate" information. DNA is more similar to CSLI than it is to the bank records in *Miller* or the pen register in *Smith*, and thus warrants an exception to the third-party doctrine. Applying the

166. *See, e.g.*, *id.* at 2220; Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

167. *See Ancestry Terms and Conditions*, ANCESTRY, https://www.ancestry.com/cs/legal/termsandconditions#AddlTerms [https://perma.cc/BMV6-S3JM] (Sept. 23, 2020); GEDMATCH, *supra* note 29; *Terms of Service*, 23ANDME, https://www.23andme.com/about/tos/ [https://perma.cc/L3TZ-ZU28] (Sept. 30, 2019). The courts have historically recognized consent for a search of property when a co-owner consents without the other owner present. Georgia v. Randolph, 547 U.S. 103, 121–22 (2006). However, if the other owner is present and objects, the objection governs. *Id.* There are a number of issues with consent in the consumer DNA context because it is unclear under *Carpenter* whether genetic relatives affirmatively consent to law-enforcement access, and with no mechanism for objections, if such consent is even valid. For an analysis of these consent issues, see Dery, *supra* note 14, at 128–34.

Carpenter factors to DNA yields the same result as it did with CSLI: a search has occurred under the Fourth Amendment.

a. Time

Time is a substantial consideration in retaining a person's DNA. DNA lasts after death and remains a crime-solving tool for decades after its initial collection. Although the *Carpenter* Court was concerned with the 127 days of CSLI obtained by the police in *Carpenter* and the five years that cellular companies retain CSLI, DNA survives for much longer. Because DNA lasts far longer than the five years that CSLI is preserved, this factor highlights the need for DNA's inclusion in the *Carpenter* exception to the third-party doctrine.

b. Pervasiveness

DNA is also sufficiently pervasive to warrant Fourth Amendment protection. Like CSLI, DNA is an "insistent part of daily life."[168] It provides an organism with biological instructions that tell it how to develop, survive, and reproduce, making it absolutely essential to survival. It pervades every facet of life because it dictates a person's existence as a human being and not a different organism. In many ways, it is even more pervasive than a cell phone because it goes with a person wherever she goes—even to the grave. People may forget their cell phones from time to time or even actively choose to leave them behind, but the body does not forget its DNA, even after death. This was exactly the issue in *Carpenter*, where the Court compared people's willingness to leave a car but seeming inability to leave their cell phones too far out of reach.[169] Applying the Court's words, DNA is "indispensable to participation in modern society"—or *any* society—because people take it with them everywhere, and they would cease to exist without it.[170] This factor weighs for DNA's protection.

c. Other Information Revealed

In addition to time and pervasiveness, DNA reveals other private information related to a person's lifestyle. Not only can DNA be used for identification purposes because it is unique between individuals, but SNPs can also reveal a person's sex, physical appearance, medical conditions, genetic history, and ancestral origin. This information is similar to the Court's concern with personal affiliations in *Carpenter* when it noted that it was

168. *Carpenter*, 138 S. Ct. at 2220 (quoting Riley v. California, 573 U.S. 373, 385 (2014)).
169. *Id.* at 2218.
170. *Id.* at 2220.

problematic under the Fourth Amendment that CSLI could reveal "familial, political, professional, religious, and sexual associations."[171] Therefore, this factor again weighs for the protection of DNA.

d. DNA Is Protected

Because all the *Carpenter* factors weigh for protection, warrantless law-enforcement access to DTC databases falls within the exception to the third-party doctrine. As a result, a court would then have to consider whether that search was reasonable.

B. Familial Searching of Consumer DNA Databases Is Unreasonable Under King

Despite the finding of a search, this fact alone does not make law-enforcement conduct violative of the Fourth Amendment.[172] If the search is justified because it is reasonable, no warrant is required. To determine if a search is reasonable, a court must balance legitimate government interests with the privacy interest of the individual searched. Applying the *King* framework to DNA in DTC databases, a court will likely conclude that a defendant's privacy interest in his DNA outweighs law enforcement's interests because the defendant is not in custody, and there are no considerations outside of criminal investigation justifying the search.

Although familial DNA cases do not involve a physical intrusion because the suspect himself has not been intruded upon, significant privacy concerns are still present because of the information revealed by SNPs. Unlike the public databases based on STR matching, DTC databases contain much more information. Because of the unique nature of SNP testing, this practice is unlike that at issue in *King*. Quite strikingly, the *King* Court addressed this issue by leaving open the question of whether purposes other than identification would bring the practice within the Fourth Amendment. Moreover, the *Carpenter* Court found that the nature of CSLI was so intimate that it warranted an exception to a long-established legal doctrine; as discussed above, DNA is arguably even more intimate than CSLI. Therefore, the factual dissimilarities between King's situation and the Court's explicit concerns about information revealed through DNA show that the DTC

171. *Id.* at 2217 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

172. *See* Maryland v. King, 569 U.S. 435, 446–47 (2013).

database issue "present[s] additional privacy concerns" that are greater than those in *King*.[173]

Despite substantial individual privacy interests, law enforcement may argue that circumstances exist to justify the search, making it reasonable. Perhaps the strongest interest is the one in public safety and solving cold cases. Of the few states that allow familial DNA testing, all restrict its use to cases that involve violent crimes, public safety risks, or the exhaustion of all leads, as was the case with the Golden State Killer and John D. Miller. Although the *Carpenter* Court noted that a law-enforcement motive that was solely "to discover evidence of criminal wrongdoing" would not make a search reasonable, the same argument could have been made in *King*.[174] In his dissent, Justice Scalia was concerned with this exact issue,[175] but the majority was more focused on law enforcement's interest in arrestee identification, even if it happened to result in a criminal conviction.[176] In the DTC database context, the government could easily make the argument that the identification of violent criminals, which would likely not occur without the use of these databases, outweighs the individual's privacy interest. The government could likewise argue that even if the third-party doctrine does not apply (and there is a Fourth Amendment search), there might be a lessened privacy interest because the information has been shared with others, thus allowing the law-enforcement interest to prevail on the balancing analysis.

Although law enforcement's interest in identification is implicated when police search DTC databases, there are two crucial distinctions: (1) the suspect is not under arrest when the search is conducted, so there is no diminished privacy interest; and (2) DTC databases reveal more information than CODIS matches. Thus, this issue is distinct from *King*. Although the government may argue that its interest outside of "*ordinary* criminal wrongdoing"[177] is identification of *particularly* violent criminals when all leads have been exhausted, at the heart of the issue is that the police need the familial DNA match to solve a crime. There is no underlying need to assess flight risk or dangerousness or to determine identification for arraignment. The sole purpose is to find "evidence of . . . wrongdoing."[178] That is clearly distinct from *King*. Moreover, the plethora of procedural protections that

173. *Id.* at 465.

174. *Carpenter*, 138 S. Ct. at 2221 (quoting Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995)).

175. *See King*, 569 U.S. at 480–82 (Scalia, J., dissenting).

176. *See id.* at 449, 460–61 (majority opinion).

177. *Id.* at 463 (emphasis added) (quoting City of Indianapolis v. Edmond, 531 U.S. 32, 38 (2000)).

178. *Id.*

were provided under the Maryland statute are not present in the DTC database context: there are no similar protections against law-enforcement use. Legally, absent company policies, the police have free rein over what they may recover from the databases and the purposes it is used for—massively different than the Maryland statute.[179] Consequently, the countervailing facts in *King* diminishing the defendant's privacy interest are not present in the DTC-database context, rendering a warrantless search unreasonable.

C. Despite Substantial Privacy Interests, Defendants Cannot Enforce Their Rights Because They Lack Standing

Although there are substantial arguments that familial searching in DTC databases violates the Fourth Amendment, it is doubtful that a defendant would ever have standing to challenge the evidence in court. Standing requires that the defendant's own rights be invaded. With familial searching, law enforcement does not search for the defendant's own DNA in the databases but his genetic relative's. Although the defendant has a reasonable expectation of privacy in his *own* DNA, as established above, it is doubtful that a court would extend such a right to *his genetic relative's* DNA, which is necessary to have standing. This lack of protection is problematic because despite DNA containing very sensitive information that would likely qualify for protection under *Carpenter* and *King*, courts cannot exclude the evidence because a defendant will not have standing to protect his privacy interest that lives in another's DNA.

Compounding this issue is the sheer number of DNA profiles contained in both public and private databases. Because a defendant lacks standing to bring a Fourth Amendment claim, law enforcement would have almost unlimited access to these samples, with the only limits being company policies. Not only would the government have access to the NDIS database, which contains nearly twenty million samples, but it would also have access to the staggering number of profiles in private databases. With both systems available, encompassing about fifty million DNA samples,[180] and with GEDmatch serving to consolidate all the private samples into one database,

179. Although some companies have tried to limit law-enforcement access to databases through user agreements, police can still "create a typical user account and upload DNA from a crime scene, circumventing the terms of service." Jason Tashea, *Genealogy Sites Give Law Enforcement a New DNA Sleuthing Tool, but the Battle over Privacy Looms*, ABA 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 [https://perma.cc/Z4JG-MQFB].

180. This figure includes twenty million in the public databases and thirty million in the private databases. *See supra* notes 18, 37.

law enforcement could have access to almost *anyone's* DNA—either directly or through a familial match. In a world without constitutional or legislative protection of genetic privacy, such an outcome would not be a matter of "if"—but "when."

D. Legislative Action Is Needed To Protect the Privacy Interests of Millions

Legislatures should address this lack of protection by creating a privacy right in an individual's DNA. A right to privacy—control over a person's genetic material—would allow people to shield their personal genetic information from government intrusion, which is a function the Fourth Amendment simply cannot serve in the current state of the law. A right to control simply means the government should not be able to have warrantless access to a person's DNA. However, as with any other legal right—constitutional or otherwise—where a right is provided, it can be waived. A legislative right to control personal genetic information could be waived by submitting DNA to a DTC database. But, as with other rights, one person's waiver does not waive for another. If the police were to run a DNA search in a DTC database that revealed a familial connection, they would be invading the defendant's privacy right because he would have a privacy interest in protecting his genetic information from unwarranted government intrusion—a right that would have been waived by the other family member. Because the defendant would have had his privacy right invaded, he would have standing under the Fourth Amendment. Therefore, a legislative right to privacy would protect the liberty of consumers to waive their rights as well as defendants' privacy interests. In fact, such a right would benefit *anyone* who wishes to keep their genetic information away from the prying eyes of the government—not just defendants.

A right to genetic privacy benefits everyone. Although a handful of defendants might be able to have the evidence against them excluded, the benefit would be a deterrent effect that would protect society as a whole. The Supreme Court has repeatedly articulated that the policy principle underlying the Fourth Amendment's exclusionary rule is deterrence: the rule's purpose is to *deter* law enforcement from conducting unlawful searches against people, whether innocent or guilty.[181] By excluding the only benefit law

181. *See, e.g.*, United States v. Janis, 428 U.S. 433, 446 (1976) ("[T]he 'prime purpose' of the rule, if not the sole one, 'is to deter future unlawful police conduct. . . . [T]he [exclusionary] rule is a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect, rather than a personal constitutional right of the party aggrieved.'"

enforcement derives from unlawful searches—evidence to be used in a criminal trial—law enforcement is left with no reason to invade *anyone's* Fourth Amendment rights, not just criminal defendants'. An innocent person's name would not end up in a law-enforcement family tree[182] if law enforcement was deterred from conducting the search at all. Even more, a right to privacy would not just protect against invasion by law enforcement. It would also protect against any type of government invasion for any purpose, like to collect personal health information[183] or track familial associations.[184] One can only imagine what the government would want with or could do with the personal genetic information of millions. Creating a right to genetic privacy would avoid such significant government access, at least without a warrant.

Therefore, a right to genetic privacy would be simple. It would provide control over personal genetic information. And how an individual would exercise that control would be left to personal choice. But providing that choice is essential to protecting privacy. Moreover, a right to genetic privacy would create Fourth Amendment standing, which would engrain genetic privacy into the constitutional scheme. Such protection would align the law with widely accepted beliefs about privacy and the protection the Constitution is supposed to provide. Although standing has always sought to limit legal remedies to the person whose rights were invaded, in the case of DNA and DTC databases, such rights do not yet exist in the DNA of another—despite the *Carpenter* Court's willingness to recognize a broader definition of privacy in the face of intimately sensitive information. Because no relief exists in the courts, however, it is the legislatures' duty to recognize

---

(quoting United States v. Calandra, 414 U.S. 338, 347–48 (1974)); United States v. Peltier, 422 U.S. 531, 536 (1975) ("[T]he Court has relied principally upon the deterrent purpose served by the exclusionary rule."); Stone v. Powell, 428 U.S. 465, 486 (1976) ("The primary justification for the exclusionary rule then is the deterrence of police conduct that violates Fourth Amendment rights.").

182. *See supra* note 9.

183. States are already collecting health information outside of the DNA context. For more information on state prescription-drug monitoring program databases, which catalogue the public's prescription data, see Jennifer D. Oliva, *Prescription-Drug Policing: The Right to Health-Information Privacy Pre- and Post-*Carpenter, 69 DUKE L.J. 775 (2020).

184. In 2018, the Department of Homeland Security purchased consumer CSLI for $25,000 from an app provider. Editorial, *Apps Are Selling Your Location Data. The U.S. Government Is Buying.*, WASH. POST (Feb. 9, 2020, 12:10 PM), https://www.washingtonpost.com/opinions/apps-are-selling-your-location-data-the-us-government-is-buying/2020/02/09/9d09475e-49e2-11ea-b4d9-29cc419287eb_story.html [https://perma.cc/N39S-RAQT]. Although the agency has not explicitly said what the information will be used for, the *Washington Post* noted "how simple it is to connect a dot to the person it represents . . . [including] an undocumented mother recently arrived from Mexico." *Id.*

the inherent privacy interest in DNA and grant individuals protection from unrestrained government access to their personal genetic information.

The legislative solution explained above would create standing for defendants to ask courts to exclude certain evidence at trial. That evidence would include the DNA match obtained from a DTC database and any other evidence that was obtained because of that initial familial match. However, although defendants should have their rights protected in court—the protection of which would further deter unlawful law-enforcement conduct against everyone—that is not to say that genetic genealogy should not be used to solve crime. Instead, it *should* be used to solve crime—but in a way that protects personal privacy. The answer to balancing these two interests lies in the text of the Fourth Amendment: a warrant issued upon a showing of probable cause.[185]

As articulated in the text of the Amendment, courts have the power to allow otherwise-protected searches upon a showing of probable cause. In the context of DTC databases, such a showing could include information derived from the unknown suspect's DNA sample and witness descriptions of the suspect's appearance or sex. The issuing warrant could then be limited to only those samples matching the suspect's description or characteristics in his DNA. Such a practice would protect samples unrelated to the crime at issue. Although this may seem tenuous, a court in Florida did just that, issuing a warrant to allow law enforcement access to GEDmatch's database, *including* those individuals who had opted out of such access.[186] In that case, using the warrant process proved *better* for law enforcement: the process allowed for broader access to the database than would have been available without the warrant. When the evidence is strong enough, police can continue to solve these terrible crimes, and privacy can be protected by requiring probable cause. The warrant process protects the privacy rights of individuals, both defendants and database users, while also providing an avenue to bring closure in these cases.

185. Another potential argument would be that countervailing circumstances justify the search, making it reasonable.

186. Kashmir Hill & Heather Murphy, *Your DNA Profile Is Private? A Florida Judge Just Said Otherwise*, N.Y. TIMES (Dec. 30, 2019), https://www.nytimes.com/2019/11/05/business/dna-database-search-warrant.html [https://perma.cc/M8PS-7LFH] ("[A] Florida detective announced at a police convention that he had obtained a warrant to [search] GEDmatch and . . . its full database . . . .").

CONCLUSION

Although advances in DNA testing have made it possible to solve some of the coldest criminal cases, these advances come at a cost to both the innocent and the guilty. There are significant privacy interests embedded in one's biological makeup, revealed through DNA. Not only does the strength of the privacy interest in DNA justify an exception to the third-party doctrine, but it also outweighs the legitimate law-enforcement interest in apprehending violent criminals. Likewise, the privacy interest in DNA warrants distinction from the Court's holding in *King* because of the more intimate nature of SNP testing and the full expectation of privacy not present while in police custody.

Despite the substantial privacy interests at risk from familial searching in DTC databases, under current law, defendants will have difficulty meeting standing requirements to challenge such action under the Fourth Amendment and have the evidence excluded. It thus rests with legislatures to develop a legal right to genetic privacy, which would not only protect the information from the government but also create a constitutional safeguard in the Fourth Amendment by establishing standing. A right to genetic privacy would protect privacy interests and allow consumers the liberty to have their DNA analyzed by Ancestry or 23andMe, both of which provide valuable services. Perhaps most importantly, however, such a right would not only protect privacy but also keep the warrant process open for law enforcement to continue to use these databases—undeniably groundbreaking crime-solving tools—to solve crimes and bring closure in the coldest of cases.