PERSONAL GENETIC TESTING AND THE FOURTH AMENDMENT

Ayesha K. Rasheed[*]

Operating under sparse regulatory oversight, direct-to-consumer ("DTC") genetic testing is rife with legal and bioethical issues involving data privacy, scientific accuracy, and consent. Meanwhile, despite several instances of misidentification, police have used genetic testing data to find and prosecute suspects such as the Golden State Killer ("Killer"), and are increasingly keen to access DTC companies' massive private databases.

The Fourth Amendment's protections against unreasonable searches and seizures would typically temper government use of individuals' genetic material. But in justifying such searches, the government can invoke the "third-party doctrine," which allows it to obtain data without a warrant when a suspect has voluntarily given that data to a third party. The growing popularity of DTC genetic testing and of police skill in wielding investigative genealogy ensure that many people—if not, someday soon, all people—can be identified and tracked by the government even if they themselves never complete a genetic test.

Though the Supreme Court recently revisited the third-party doctrine in Carpenter v. United States, it neither overhauled the doctrine to accommodate the vast data-gathering capabilities of modern technology, nor resolved pre-existing doctrinal confusions. Carpenter's application to DTC genetic data is therefore unclear. This Article is among the first to examine whether third-party doctrine exempts DTC genetic data from Fourth Amendment protections. It argues that the doctrine's premises, both before and after Carpenter, ill-fit genetic data's hypersensitive attributes and questionable DTC industry practices. DTC DNA data thus reveals a fundamental flaw in the Court's conception of the third-party doctrine: namely, its failure to recognize a burgeoning category of information that is generated, at least in part, by third parties, and the contents of which are not fully known to individuals when they share it. A strict warrant requirement for police searches of DTC genetic data is an essential first step for ensuring that such searches conform to the Fourth Amendment right to privacy.

[*] J.D. Candidate, University of California, Berkeley, School of Law; M.Sc., University of Oxford; B.S. with Honors, Stanford University. First, a thousand thanks to Professor Andrea Roth of Berkeley Law for her invaluable edits and support throughout the writing process. Special thanks also to Jeremy Isard, for helping me hone an early draft, and my parents, for everything. I am also grateful to Professor Tejas Narechania of Berkeley Law and friends at the *California Law Review* for their feedback. Errors and oversights are my own.

TABLE OF CONTENTS

I. INTRODUCTION

The Golden State Killer's twelve-year spree of rape, murder, and burglary left behind hundreds of victims and over 10,000 pages of case files across at least nine California counties.[1] For forty-four years, however, the Killer eluded authorities.[2] Despite an apparent abundance of data, "criminal DNA databases produced no hits, sweeps of crime scenes no fingerprints and hefty rewards no definitive tips."[3] Then, in early 2018, genetic testing results from the Killer's distant relatives ended the impasse.[4] Using DNA from a long-cold murder scene, investigators were able to identify the Killer's great-great-great grandparents from the 1800s via an online genetic testing database called GEDmatch.[5] Those

1. *See* Redacted Search Warrant and Affidavit of Detective Robert Peters, People v. Joseph James DeAngelo, No. 18FE008017 (Cal. Sup. Ct. Cty. Sacramento April. 24, 2018), http://goldenstatekillertrial.com/files/warrant.pdf.

2. Justin Jouvenal, *To Find Alleged Golden State Killer, Investigators First Found His Great-Great-Great-Grandparents*, WASH. POST (April 30, 2018, 5:22 PM), https://www.washingtonpost.com/local/public-safety/to-find-alleged-golden-state-killer-investigators-first-found-his-great-great-great-grandparents/2018/04/30/3c865fe7-dfcc-4a0e-b6b2-0bec548d501f_story.html?utm_term=.5e40e148c19d.

3. *Id.*

4. *Id.*

5. *Id.*

individuals were analyzed to create a family tree, one branch of which led law enforcement to the door of Joseph James DeAngelo.[6] At seventy-two, DeAngelo is now being tried on twenty-six charges.[7]

Law enforcement officers have also identified other criminal suspects using investigative genealogy—or so we thought.

Several less-publicized stories illustrate investigative genealogy gone awry. Before police arrested DeAngelo, for instance, they incorrectly identified a bed-ridden man in Oregon as a genetic match to the Golden State Killer's DNA.[8] Likewise, three years prior, Idaho Falls police used similar methods to arrest New Orleans filmmaker Michael Usry Jr. for the brutal 1996 murder of teenager Angie Dodge.[9] Subsequent DNA testing, however, helped prove Usry's innocence.[10]

The police's creative use of a pool of genetic information beyond that of convicted felons[11] indicates it will next seek access to private direct-to-consumer ("DTC") genetic databases. Law enforcement use of investigative genealogy has surged since DeAngelo's arrest in the Golden State Killer case, resulting in the arrest of at least twenty-seven suspects in other cases over the remainder of 2018.[12] Indeed, in February of 2019, genetic testing company FamilyTreeDNA disclosed an agreement that allows the Federal Bureau of Investigation ("FBI") to test DNA samples against its database of nearly two million customers.[13]

Combined with genetic data's ability to provide powerful evidence of guilt or innocence through techniques such as DNA profile matching,[14] access to DTC genetic testing data would give the government more information about more people than it has ever previously been able or authorized to reach. Like any

6. *See* Ryan Lillis et al., *'Open-Source' Genealogy Site Provided Missing DNA Link to East Area Rapist, Investigator Says*, SACRAMENTO BEE (Apr. 27, 2018, 11:03 AM) https://www. sacbee.com/news/local/crime/article209987599.html.

7. First Amended Complaint, People v. Joseph James DeAngelo, No. 18FE008017 (Cal. Sup. Ct. Cty. Sacramento).

8. *See* Michael Balsamo et al., *Police Using Genetic Sites Misidentified Oregon Man as Golden State Serial Killer Suspect in 2017*, CHI. TRIB. (Apr. 28, 2018, 9:39 AM), https://www.chicagotribune.com/news/nationworld/ct-genealogy-site-serial-killer-20180427-story.html.

9. *See* Anne-Marie Green et. al, *Who Murdered Idaho Teen Angie Dodge?*, CBS NEWS: 48 HOURS (Dec. 15, 2017), https://www.cbsnews.com/news/the-dna-of-a-killer-who-murdered-idaho-teen-angie-dodge/.

10. *See* EastIdahoNews.com Staff, *DNA Report Clears Usry Family of Involvement in Angie Dodge Homicide Case*, EAST IDAHO NEWS (July 12, 2017, 9:19 AM), https://www.eastidahonews.com/2017/07/dna-report-clears-usry-family-involvement-angie-dodge-homicide-case/ (detailing how police searches of Ancestry.com indicated Usry matched 34 of 35 markers from the suspect's DNA, but subsequent testing by Parabon Nanonlabs cleared the Usry family "out to the 6th-degree relative" with 87.63% confidence).

11. That is, GEDmatch's repository for the results of genetic tests processed elsewhere. *See, e.g.*, *id.*

12. *See* Robert Gearty, *DNA, Genetic Genealogy Made 2018 the Year of the Cold Case: 'Biggest Crime-Fighting Breakthrough in Decades'*, FOX NEWS (Dec. 19, 2018), https://www.foxnews.com/us/dna-genetic-genealogy-made-2018-the-year-old-the-cold-case-biggest-crime-fighting-breakthrough-in-decades.

13. *See* Kristen V. Brown, *Major DNA Testing Company Sharing Genetic Data With the FBI*, BLOOMBERG (Feb. 1, 2019, 4:23 PM), https://www.bloomberg.com/news/articles/2019-02-01/major-dna-testing-company-is-sharing-genetic-data-with-the-fbi.

14. Henry T. Greely, *"Who Knows What Evil Lurks in the Hearts of Men?": Behavioral Genomics, Neuroscience, Criminal Law, and the Search for Hidden Knowledge, in* THE IMPACT OF BEHAVIORAL SCIENCES ON CRIMINAL LAW 161, 172 (Nita A. Farahany ed., 2009).

technology, however, genetic genealogy is imperfect. And in the criminal justice context, the consequences of police mistakes or overreach are high. DeAngelo, for example, if convicted of murder, faces the possibility of the death penalty or life imprisonment—and even if acquitted at trial, his name has become irrevocably entwined with the case.[15]

The scale of source expansion would be dramatic.[16] The number of people whose genetic data can be found through DTC databases is growing exponentially, not only because of the popularity of DTC testing (see Table 1), but also because of familial relationships that can be inferred.[17] In 2017, AncestryDNA sold 1.5 million kits over Black Friday weekend alone,[18] and the consumer market for DTC genetic tests is predicted to triple from $99 million in 2017 to at least $310 million in 2022.[19] As of early 2018, industry estimates show that at least 1 in 25 Americans have used DTC genetics services,[20] and 15% of the U.S. population has taken a genetic test of some kind.[21]

15. *See Golden State Killer Suspect May Face Death Penalty*, CBS DENVER (Apr. 17, 2019, 1:43 PM), https://denver.cbslocal.com/2019/04/17/joseph-deangelo-golden-state-killer-suspect-may-face-death-penalty/ (reporting prosecutors' in-court statements that they will seek the death penalty in DeAngelo's trial, despite the California governor's moratorium on executions).

16. Legal scholars have shown that existing DNA databases used by law enforcement are also overbroad and poorly maintained, *see, e.g.*, ERIN E. MURPHY, INSIDE THE CELL: THE DARK SIDE OF FORENSIC DNA (2016). That DTC DNA databases dwarf pre-existing police databases in size thus amplifies the need to scrutinize Fourth Amendment protections in this context.

17. Megan Molteni, *Ancestry's Genetic Testing Kits Are Heading for Your Stocking This Year*, WIRED (Dec. 1, 2017, 7:00 AM), https://www.wired.com/story/ancestrys-genetic-testing-kits-are-heading-for-your-stocking-this-year/; Antonio Regalado, *More Than 26 Million People Have Taken an At-Home Ancestry Test*, MIT TECH. REV. (Feb. 11, 2019), https://www.technologyreview.com/s/612880/more-than-26-million-people-have-taken-an-at-home-ancestry-test.

18. Molteni, *supra* note 17.

19. KALORAMA INFORMATION REPORT: THE MARKET FOR DIRECT-TO-CONSUMER GENETIC HEALTH TESTING (2018), https://www.kaloramainformation.com/Direct-Consumer-Genetic-Health-Testing-11370673/.

20. Antonio Regalado, *2017 Was the Year Consumer DNA Testing Blew Up*, MIT TECH. REV. (Feb. 12, 2018, 7:00 AM), https://www.technologyreview.com/s/610233/2017-was-the-year-consumer-dna-testing-blew-up/.

21. Jeff Roberts, *Mapping the Future*, BEST'S REV. 48, 49 (June 2018), https://www.swissre.com/dam/jcr:e07a4939-6746-430e-9be8-00009f4774c5/2018_map_future_genomics.pdf. Also, as Part III discusses, the growing percentage of Americans using DTC testing services do not represent the general population's diversity. Rather, the majority of individuals using DTC genetic testing services are Caucasians of European descent. Lack of diversity has hindered research, particularly into the efficacy of drugs, and prompted waves of advertising campaigns by DTC companies to target underrepresented races and ethnicities. *See* Sarah Zhang, *23andMe Wants Its DNA Data to Be Less White*, ATLANTIC (Apr. 23, 2018), https://www.theatlantic.com/science/archive/2018/04/23andme-diversity-dna/558575/ (examining ethical issues raised by 23andMe's offer of free spit kits to researchers studying populations in Africa and Asia). Many past and present efforts to increase sample diversity in genetics feature questionable research practices, if not instances of outright ethical violations. *See, e.g.* Katrina G. Claw et al., *A Framework for Enhancing Ethical Genomic Research with Indigenous Communities*, 9 NATURE COMMS. 2957, 1257–63 (July 2018).

TABLE 1: TOTAL PEOPLE TESTED* BY POPULAR DTC GENETICS COMPANIES AS OF NOV. 2018[22]

DTC Company	Estimated Total People Tested
23andMe	25 million
Ancestry	14 million
MyHeritage	2.5 million
Family Tree DNA	2 million

* Ancestry reports kit sales, not the number of tests submitted for testing.

The true number of Americans whose genetic information has been shared with commercial actors is even higher than these figures suggest.[23] DNA is familial,[24] so any individual who submits their DNA for testing also forfeits genetic data shared by all their known and unknown relatives and descendants.[25] Due to this, one university study estimates that 60% of Americans of Northern European descent can be identified through extant online genealogy databases, whether or not they uploaded their own data.[26] That figure will rise to 90% within the next two or three years.[27]

Unlike DNA testing by law enforcement, DTC genetic testing is highly sensitive because its insights go well beyond suspect identification. DTC companies advertise that their tests can reveal information such as: predisposition to disease, disease carrier status, unknown biological relatives, and Ashkenazi Jewish or Native American heritage.[28] DTC data therefore allows for hypersensitive inferences about an individual's identity or membership in a group that is a target for discrimination—such as disability status or religious preference.[29] By con-

22. Testing estimates from Antonio Regalado, *supra* note 17. These numbers also do not subtract the "small" number of users that test with more than one company.

23. *Id.*

24. Only approximately 0.1% of the human genome varies between individuals. *Genetics vs. Genomics Fact Sheet*, NAT'L HUM. GENOME RES. INST., https://www.genome.gov/19016904/faq-about-genetic-and-genomic-science/ (last visited on May 27, 2020).

25. Regalado, *supra* note 17.

26. *See* Heather Murphy, *Most White Americans' DNA Can Be Identified Through Genealogy Databases*, N.Y. TIMES (Oct. 11, 2018), https://www.nytimes.com/2018/10/11/science/science-genetic-genealogy-study.html.

27. *See id*.

28. *See, e.g.*, *What You Can Learn*, 23ANDME, https://customercare.23andme.com/hc/en-us/sections/200565460-What-You-Can-Learn (last visited May 27, 2020). Notably, in late 2018, Senator Elizabeth Warren (D-Mass) used a genetic test to show "strong evidence" of her Native American ancestry. The Stanford professor who authored her report, Carlos Bustamante, advises both Ancestry and 23andMe. Many decried Warren's genetic test as a publicity stunt that inappropriately simplified difficult debates about how Native American identity is determined. The Cherokee Nation, which Warren claims an ethnic connection to, rebuked Warren directly, stating that using a "DNA test to lay claim to any connection to the Cherokee Nation or any tribal nation, even vaguely, is inappropriate and wrong" because it risks "dishonoring legitimate tribal governments and their citizens" and "undermining tribal interests." See Asma Khalid, *Warren Releases DNA Results, Challenges Trump Over Native American Ancestry*, NPR (Oct. 15, 2018, 11:44 AM) https://www.npr.org/2018/10/15/657468655/warren-releases-dna-results-challenges-trump-over-native-american-ancestry; Zak Cheney-Rice, *Elizabeth Warren's Native American Ancestry Was Never Really the Point*, INTELLIGENCER (Oct. 15, 2018) http://nymag.com/intelligencer/2018/10/elizabeth-warrens-native-ancestry-was-never-the-point.html.

29. *See What You Can Learn*, *supra* note 28.

trast, genetic markers maintained in existing police databases and used for forensic testing serve almost exclusively as a means of identification.[30] The Supreme Court has, for that reason, referred to existing police DNA databases as "no more than an extension of methods of identification long used in dealing with persons under arrest" such as fingerprinting.[31] As this Article explains, the same cannot be said for DTC genetic testing data.

Though growing concerns over genetic privacy have led many DTC companies to pledge to resist turning over customers' data to police,[32] such promises ring hollow in light of the lack of statutory protections. DTC companies operate under a threadbare regulatory regime with little oversight.[33] And, because most companies offer a range of testing services,[34] what regulation there is often fails to delineate who should enforce it.[35] As it stands, DTC genetic testing is virtually unchecked in the realms of quality control, data privacy, data security, and consumer protection.[36] So, while industry leader 23andMe, for example, offers a "Guide for Law Enforcement" that sets out limits for law enforcement officers requesting user data,[37] no statute guarantees those limits.[38] The result is that for-profit DTC companies have a financial incentive and no regulatory obstacles to expand services, amass vast quantities of genetic records, and use and sell the personal data they harvest to other companies, government agencies, and the like.[39]

Even in the absence of regulation, police use of sensitive genetic material would presumably trigger constitutional protections in the form of the Fourth Amendment's guarantee against unreasonable searches and seizures.[40]

The third-party doctrine, however, holds that Fourth Amendment protections are void when an individual voluntarily shares their data with a third

30. Madison Pauly, *Police Are Increasingly Taking Advantage of Home DNA Tests. There Aren't Any Regulations to Stop It*, MOTHERJONES (Mar. 12, 2019), https://www.motherjones.com/crime-justice/2019/03/genetic-genealogy-law-enforcement-golden-state-killer-cece-moore/.

31. *See* Maryland v. King, 569 U.S. 435, 461 (2013) (quoting United States v. Kelly, 55 F.2d 67, 69 (2d Cir. 1932)).

32. *See, e.g.*, *Transparency Report*, 23ANDME, https://www.23andme.com/transparency-report/ (last visited May 27, 2020).

33. Kathy Hudson et al., *ASHG Statement on Direct-to-Consumer Genetic Testing in the United States*, 82 AM. J. HUM. GENETICS 635, 635 (2007).

34. Andelka M. Phillips, *Only A Click Away—DTC Genetics for Ancestry, Health, Love…and More: A View of the Business and Regulatory Landscape*, 8 APPLIED & TRANSLATIONAL GENOMICS 16, 17 (2016) (grouping services offered by DTC genetics companies into the following categories and noting that over half the companies surveyed offer services in multiple categories: health testing, carrier testing, nutrigenic testing, ancestry, genetic relatedness, athletic ability, child talent, surreptitious testing (so-called "infidelity" tests and paternity tests), and matchmaking).

35. *See generally* Hudson et al., *supra* note 33.

36. *See* Philips, *supra* note 34, at 20.

37. *23andMe Guide for Law Enforcement*, 23ANDME, https://www.23andme.com/law-enforcement-guide/ (last visited May 27, 2020) (announcing that 23andMe's policy is to "use all practical legal and administrative resources to resist requests from law enforcement" and "not share customer data with any public databases, or with entities that may increase the risk of law enforcement access").

38. *See* George J. Annas & Sherman Elias, *23andMe and the FDA*, 370 NEW ENG. J. MED., 985, 985 (2014).

39. *See id.* at 986–87.

40. *See generally* Catherine W. Kimel, Note, *DNA Profiles, Computer Searches, and the Fourth Amendment*, 62 DUKE L.J. 933 (2013).

party.[41] Here, because customers give their saliva samples to DTC companies, the third-party doctrine seemingly allows the government to access DTC DNA databases without first obtaining a warrant based on probable cause.[42] Because industry leaders have promised to resist law enforcement efforts to obtain their data[43] at the very instant that police have found new uses for it, invoking third-party doctrine may be law enforcement's quickest way to get genetic testing data.[44]

This Article is among the first to analyze the legality and desirability of law enforcement use of DTC genetic testing databases against the backdrop of the Fourth Amendment. As of this Article's publication, no court has addressed whether and to what extent the Fourth Amendment protects DNA data collected by DTC companies, despite the scale and hypersensitivity of the data at issue. I argue that DTC genetic data should be exempt from the third-party doctrine and that current conceptions of the doctrine are flawed.[45] Building upon the Supreme Court's opinion in *Carpenter*, which probed whether the third-party doctrine applied to stored cell phone location metadata in an era when most people use cell phones constantly, this Article clarifies why the third-party doctrine should not apply to DTC data.

The argument proceeds in three parts. After describing the scientific and regulatory landscape of personal genetic testing in Part II, Part III explains doctrinal issues that complicate the Fourth Amendment's application to searches of DTC databases and thus expose central problems with the Court's attempts to delineate private things and places. Finally, Part IV crystallizes what the third-party doctrine must address if it is to survive and suggests that one way to correct it is through a warrant requirement for searches of DTC DNA data that specifies what is being searched for and takes steps to limit segments of the database searched. Part IV also surveys whether search doctrine's property law-based jurisprudence might be combined with the Court's "reasonable expectation of privacy" case law to update the doctrine for the Information Age.

II. LAW ENFORCEMENT USE OF DTC GENETIC TESTING DATABASES

Individuals' privacy interests in government access to for-profit DTC testing databases are greater than those implicated by existing police databases.[46] To explain why, this Part overviews the emergence of DTC genetic testing, its science, law enforcement use of such databases, and the dearth of legal and ethical oversight in this area.

41. John Villasenor, *What You Need to Know About the Third-Party Doctrine*, ATLANTIC (Dec. 30, 2013), https://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721/.

42. *See id.*

43. *See, e.g.*, *23andMe Guide for Law Enforcement*, *supra* note 37.

44. Villasenor, *supra* note 41.

45. *See infra* Part IV.

46. *See id.*

To that end, a primer on genetics is helpful. The human genome is encoded in double-stranded DNA molecules consisting of complementary nucleotide chains.[47] Though the human genome contains about six billion nucleotide bases (A; C; G; T), approximately 99% of any two human genomes are the same.[48] What remains constitutes the "genetic variation" that makes an individual human unique.[49] The most common type of genetic variant is a single nucleotide polymorphism ("SNP," pronounced "snip").[50] Each SNP represents a difference in a single DNA building block; for example, a SNP may replace the nucleotide cytosine (C) with the nucleotide thymine (T) in a certain stretch of DNA.[51] SNPs thus serve as genetic markers that help researchers locate genes.[52] Because SNPs "have a direct influence on our physical attributes (*e.g.*, hair color, eye color, blood type) . . . [and] predispositions to various diseases,"[53] 23andMe, Ancestry, and many other DTC genetics companies load saliva samples onto SNP chips to quickly and cheaply "spot-check" a person's sample against a preset collection of SNPs known to be involved in certain traits.[54] "[T]oday, there are approximately 50 million approved (by the research community) SNPs in the human population."[55]

A. The Emergence of DTC Genetic Testing

At low cost and with little effort, DTC genetic testing promises the public quick answers to the mysteries hidden in their DNA. For around $100,[56] personal genetic testing offers a tantalizing array of ever-expanding insights, ranging from the profound ("Where do I come from? Am I a disease carrier?") to the trivial ("Is my hatred of the sound of chewing genetically based? My aversion to cilantro?").[57] Kits are easy to use, and tidy interfaces, colorful infographics, and a reassuring aura of statistical accuracy make results seem simple and concrete.[58]

47. Mathias Humbert et al., *De-anonymizing Genomic Databases Using Phenotypic Traits*, 2 PROC. ON PRIVACY ENHANCING TECH. 99, 101 (2015).

48. *Id.*

49. *See id.*

50. *What Are Single Nucleotide Polymorphisms (SNPs)?*, U.S. NAT'L LIBR. OF MED. (Jan. 21, 2020), https://ghr.nlm.nih.gov/primer/genomicresearch/snp.

51. *Id.*

52. *Id.*

53. Humbert et al., *supra* note 47, at 101. This figure is already outdated. The number of research community-validated SNPs on the NCBI webpage has grown from approximately 50 million when Humbert referenced it in 2015 to over 335 million as of my access on 26 Sept. 2018. That webpage is located at https://www.ncbi.nlm.nih.gov/SNP/snp_summary.cgi.

54. *See* Tina H. Saey, *Your DNA Is an Open Book—But Can't Yet Be Fully Read*, SCI. NEWS FOR STUDENTS (May 24, 2018, 5:45 AM), https://www.sciencenewsforstudents.org/article/your-dna-open-book-cant-yet-be-fully-read.

55. Humbert et al., *supra* note 47, at 101.

56. *See, e.g.*, 23ANDME, https://www.23andme.com/?myg=true (last visited May 27, 2020).

57. *Health + Ancestry Service*, 23ANDME, https://www.23andme.com/dna-health-ancestry/ (last visited May 27, 2020).

58. *See, e.g.*, *How 23andMe Personal Genetic Service Works*, 23ANDME, https://customercare.23andme.com/hc/en-us/articles/227968028-How-23andMe-works (last visited May 27, 2020) (describing how a typical DTC genetic testing kit works: individuals place about 2 mL of clean saliva in the provided tube, add pre-mixed

But the groundbreaking product offered by DTC companies like 23andMe has never been the report that customers receive in the mail. The real product, dear reader, is you. With astonishing success, at least 246 companies[59] have amassed the DNA of millions of individuals since the technology's introduction in the early 2000s.[60] That trove of data enables myriad activities of considerable commercial and scientific value, including research, sales of consumers' data to third parties like pharmaceutical companies, and, as this Article will discuss, problematic use by law enforcement agencies.[61]

DNA testing went mainstream following the landmark completion of the Human Genome Project in 2003, as companies hurried to exploit the Project's scientific breakthroughs.[62] The Project fully sequenced the human genome for the first time, taking over a decade of concerted international effort to complete.[63] Researchers and entrepreneurs hoping to mine the Project's publicly available data eagerly awaited its completion, and soon after that occurred, 23andMe established itself as the pioneer in DTC genetic testing.[64] Founded in 2006, the company capitalized on the Project's publicity and research, and aimed to "get the general public to. . . [join] their gene pool" to enable further insights.[65]

The ensuing race to expand and corner the personal genetic testing market made DTC testing cheaper and more accessible. In 2007, 23andMe introduced its first direct-to-consumer spit kit: a $999 "Personal Genome Service" that offered "insights into a person's disease risk, ethnic ancestry, and other traits, among them their sensitivity to certain tastes."[66] Despite the steep price tag, "competitors piled into the market, most prominently AncestryDNA, a subsidiary of Ancestry.com."[67] Counter-competition, in turn, led 23andMe to slash its kits' prices to $99-199, setting the current industry standard.[68] Decreasing testing prices are also likely to occur with whole genome sequencing, which sequences an individual's entire genetic code as opposed to DTC tests' pre-chosen

stabilization buffer, then mail their sample to a company laboratory using a pre-paid envelope. Customers must then create an online profile, from which they can later access their results and infographics).

59. *See* Phillips, *supra* note 34, at 17 (listing DTC companies offering online services as of January 2016, based upon work by the Human Genetics Commission, U.S. Government Accountability Office, and Johns Hopkins Genetics and Public Policy Center).

60. George Whaley & Stephen McGuire, *23andMe: Future of Personal Genomics Services Business?*, 36 J. CASE STUD. 78, 78–79 (2018).

61. *See infra* Section II.B.

62. *See* Drake Bennett & Kristen V. Brown, *Your DNA Is Out There. Do You Want Law Enforcement Using It?*, BLOOMBERG BUSINESSWEEK (Oct. 27, 2018), https://www.bloomberg.com/news/features/2018-10-27/your-dna-is-out-there-do-you-want-law-enforcement-using-it; *Human Genome Project Fact Sheet*, NAT'L INST. HEALTH, https://archives.nih.gov/asites/report/09-09-2019/report.nih.gov/nihfactsheets/ViewFactSheet cd22.html?csid=45 (last visited May 27, 2020).

63. *See Human Genome Project*, *supra* note 62.

64. Whaley & McGuire, *supra* note 60, at 83.

65. *Id.* at 78; 23ANDME, *About Us*, https://mediacenter.23andme.com/company/about-us/ (last visited May 27, 2020).

66. *See* Bennett & Brown, *supra* note 62.

67. *Id.*

68. Luke Tillerman, *23andMe Brings Down the Price of Consumer Genetic Tests, Builds Up Relations With Big Pharma*, XCONOMY (May 24, 2011), https://xconomy.com/san-francisco/2011/05/24/23andme-moves-beyond-simple-consumer-dna-sequencing-sets-sight-on-research/.

code segments.[69] Veritas—the market leader for whole genome sequencing—does its sequencing on machines manufactured by biotechnology company Illumina, and Illumina is expected to drop its sequencing prices in response to pressure from Chinese competitor BGI.[70] Both genotyping and whole genome sequencing costs should drop further as data storage and information extraction become easier.[71]

Nascent regulatory repartee over medical usage distracts from DTC companies' chief aim: amassing private, profitable genetic biobanks.[72] Companies are willing to offer expensive testing services at a significant consumer discount in order to collect valuable genetic data.[73] Individually, for example, the cost of a paternity test ranges from $69 to $399, while testing for the presence of breast cancer risk genes *BRCA1* and *BRCA2* ranges from $300 to $5,000.[74] Both services, however, are available in a basic form via popular 23andMe kits that retail for a mere $99.[75] Companies justify these steep discounts because ultimately, they often leverage their databases for research or sell access onwards in hopes of leading to patentable discoveries.[76]

Though the personal nature of consumers' insights is heavily advertised, DTC companies have always sought partnerships with other commercial actors interested in their customers' data. Companies make millions of dollars by allowing pharmaceutical, biotechnology, and technology companies, among others, to use their data. 23andMe, for example, has signed contracts with pharmaceutical giants Genentech and Pfizer,[77] and, netting a $300 million profit, GlaxoSmithKline.[78] Likewise, for many years AncestryDNA worked alongside

69. *See* Joe Andrews, *23andMe Competitor Veritas Genetics Slashes Price of Whole Genome Sequencing 40% to $600*, CNBC (Jul. 1, 2019, 9:30 AM), https://www.cnbc.com/2019/07/01/for-600-veritas-genetics-sequences-6point4-billion-letters-of-your-dna.html.

70. Megan Molteni, *Now You Can Sequence Your Whole Genome for Just $200*, WIRED (Nov. 19, 2018, 8:08 AM), https://www.wired.com/story/whole-genome-sequencing-cost-200-dollars/.

71. *Id.*

72. *See Top Companies in Medical Genetics*, MEDICAL FUTURIST, https://medicalfuturist.com/top-companies-genomics/ (last visited May 27, 2020).

73. Molteni, *supra* note 70.

74. Direct data on how much it costs DTC companies to run any of their various tests is kept closely guarded, thus necessitating alternative points of comparison. It may also be notable that whole-genome sequencing, which has traditionally been much more difficult than SNP testing, has decreased its cost of sequencing a single genome from just over $4,000 in 2015 to roughly $1,000 today. *See* DNA DIAGNOSTICS CENTER, https://dnacenter.com/blog/how-much-does-a-paternity-test-cost (last visited May 27, 2020), *Genetic Testing Facilities and Costs*, BREASTCANCER.ORG (June 23, 2016, 12:32 PM), https://www.breastcancer.org/symptoms/testing/genetic/facility_cost.

75. *Three Easy Ways to Discover You*, 23ANDME, https://www.23andme.com/compare-dna-tests/ (last visited May 27, 2020); *see also The Cost of Sequencing a Human Genome*, NATIONAL HUMAN GENOME RESEARCH INSTITUTE, https://www.genome.gov/27565109/the-cost-of-sequencing-a-human-genome (last visited May 27, 2020).

76. *See* G. J. Annas & S. Elias, *23andMe and the FDA,* 370 NEW ENG. J. MED., 985,987(2014); *see also* Heather Somerville, *23andMe Aims to be Google for Genetic Research*, MERCURY NEWS (Aug. 12, 2016, 5:40 AM), https://www.mercurynews.com/2014/09/ 06/23andme-aims-to-be-google-for-genetic-research/.

77. *See Research*, 23ANDME, https://www.23andme.com/research/ (last visited on May 27, 2020).

78. Bloomberg, *GlaxoSmithKline Is Acquiring a $300 Million Stake in Genetic-Testing Company 23andMe*, FORTUNE (July 25, 2018, 10:36 AM), https://fortune.com/2018/07/25/glaxosmithkline-23andme-gsk/.

Calico, a Google-backed biotech research and development venture.[79] The terms of such partnerships are often secret, so there is little transparency about how and why other corporations seek or receive access to DTC genetics data.[80]

To understand the ramifications of the lack of Fourth Amendment protections for DTC genetic databases, it is important to distinguish what kind of personal information is actually at risk of government collection through the third-party doctrine. The types of genetic markers used in DTC testing are different, and much more potentially invasive of an individual's privacy than the types of genetic markers traditionally used in law enforcement DNA databases.

"Genetic testing" is an unwieldy term that encompasses a range of tests with unique DNA sources and insights, and is often misunderstood by policymakers and the public. One particular source of confusion is slippage between the terms "genetic testing" or "genetic ancestry testing" and "familial DNA searches" or "familial searching." Brought to public attention by the Golden State Killer case,[81] familial searching compares a suspect's DNA against other individuals' DNA records to find a suspect's relatives using the "predictable way" human relatedness operates.[82] That is, of the small percentage of DNA that varies between individuals, "we share roughly half with each parent or sibling; a quarter with grandparents, aunts, uncles, and half-siblings; 12.5 percent with first cousins; 6.25 percent with our parents' first cousins; 3.13 percent with our second cousins, and so on. The ratios aren't exact . . . But there are calculable ranges."[83] Importantly, familial searching does not involve direct lab testing or sequencing of a suspect's biological sample and reveals only basic information about which individuals a suspect may be related to.[84]

In addition to confusion with familial testing, "genetic testing" is incorrectly used as a catch-all term to describe a range of DNA tests. It has been used to refer to SNP testing, Y-chromosome tests, mitochondrial DNA tests, and autosomal (*i.e.* from a numbered chromosome rather than an X or Y sex chromosome) DNA tests.[85] It has not yet been widely used to describe services that sequence a person's whole genome, but that may be because they remain too

79. Katherine Drabiak, *Caveat Emptor: How the Intersection of Big Data and Consumer Genomics Exponentially Increases Information Privacy Risks*, 27 HEALTH MATRIX, 143, 170.

80. *See* Julia Belluz, *Google Is Super Secretive About Its Anti-Aging Research. No One Knows Why*. VOX (Apr. 28, 2017, 2:35), https://www.vox.com/science-andhealth/2017/4/27/15409672/google-calico-secretive-aging-mortality-research (describing Calico as notorious for maintaining strict secrecy about its products and objectives, despite allocating vast capital stores (approximately $1.5 billion) towards research).

81. *See* Norman A. Paradis, *The Golden State Killer Case Shows How Swiftly We're Losing Genetic Privacy*, VOX (May 5, 2018, 10:24 AM), https://www.vox.com/science-and-health/2017/4/27/15409672/google-calico-secretive-aging-mortality-research (providing an overview of how law enforcement officials tracked down the Golden State Killer suspect using genetic information).

82. *See* Bennett & Brown, *supra* note 62.

83. *Id.*

84. *See* Paradis, *supra* note 81.

85. *Understanding Genetic Ancestry Testing*, U.C. LONDON, https://www.ucl.ac.uk/biosciences/understanding-genetic-ancestry-testing-0 (last visited May 27, 2020).

expensive for the average consumer.[86] This Article focuses on genotyping (*i.e.* is limited to SNPs), though it anticipates the near future when more SNPs are tested and whole-genome sequencing is commonplace.

Crucially, all these tests are much more intrusive than the forensic DNA "profiles" uploaded to the FBI's Combined DNA Index System ("CODIS").[87] Unlike DTC genetic testing, CODIS does not file a person's DNA "sample." A person's forensic profile instead "consists of her two genetic markers or 'alleles' at each of twenty 'junk DNA' locations."[88] Though controversy exists over whether the genetic markers used in forensic testing are *actually* junk sites,[89] the SNPs used in DTC testing indicate sensitive information.[90] DTC "tests are more sophisticated than the DNA tests police typically run, and they generate more data than is stored in the FBI's CODIS database."[91] But despite their different orders of magnitude of sensitivity, the term "genotyping" applies to both DTC and forensic testing.[92] SNP chips used in DTC genetic testing are sometimes known as genotyping arrays, so DTC testing is sometimes called "genotyping."[93] The same term, however, is used in the forensic context with respect to STR alleles (*i.e.* relevant junk DNA loci).[94] Allowing the government warrantless access to the more sophisticated DNA data in DTC companies' databases thus gives police far more data about individuals than the simple matches its own forensic profiles provide.

86. As has been the trend in genetics, testing costs are plummeting. For example, Veritas Genetics, which offers whole genome sequencing services, dropped its usual kit price of $999 to just $199 for the 2018 holiday shopping season. *See* Molteni, *supra* note 70.

87. *See* Andrea Roth, *'Spit and Acquit': Prosecutors as Surveillance Entrepreneurs*, 107 CALIF. L. REV. 405, 407 (2019).

88. *Id.* at n.1.

89. *See e.g.* Stephen S. Hall, *Hidden Treasures in Junk DNA*, SCI. AM. (Oct. 1, 2012), https://www.scientificamerican.com/article/hidden-treasures-in-junk-dna/.

90. *See What Are Single Nucleotide Polymorphisms (SNPs)?*, *supra* note 50.

91. Sarah Zhang, *The Coming Wave of Murders Solved by Genealogy*, ATLANTIC (May 19, 2018), https://www.theatlantic.com/science/archive/2018/05/the-coming-wave-of-murders-solved-by-genealogy/560750/.

92. *See, e.g.*, *Difference Between DNA Genotyping and Sequencing*, 23ANDME, https://customercare.23andme.com/hc/en-us/articles/202904600-Difference-Between-DNA-Genotyping-Sequencing (last visited May 27, 2020) (defining the term "genotyping").

93. Behind the Bench Staff, *Direct-to-Consumer (DTC) Genetic Ancestry Reports: Why Genotyping is Essential*, THERMOFISHER SCIENTIFIC (Jun. 13, 2019), https://www.thermofisher.com/blog/behindthebench/direct-to-consumer-dtc-genetic-ancestry-reports-why-genotyping-is-essential/.

94. *See, e.g.*, *STR Genotyping*, MOLECULAR DIAGNOSTIC SERV., http://www.mds-usa.com/strgeno.html (last visited on May 27, 2020).

B. Law Enforcement Use of Genetic Testing Databases

In recent decades, advances in genetics have elevated the role of DNA from mere supporting evidence to a powerful investigatory and prosecutorial tool.[95] Historical trends suggest that DTC DNA databases are the next source police will tap in their mounting efforts to collect and use biological data.[96]

Recent events show the acceleration of law enforcement's use of genetic databases based upon DTC testing data. Credited with killing twelve people, raping fifty-one others, and burglarizing hundreds of homes, the Golden State Killer terrorized California from about 1974 to 1986.[97] His crimes remained unsolved for over forty years, law enforcement hung on to one piece of evidence that technology eventually unlocked: DNA from an object the Killer had discarded at a murder scene.[98] In 2018, that DNA led to the arrest of former police officer Joseph James DeAngelo and his arraignment for twenty-six rape and murder charges across six jurisdictions.[99]

The crime scene DNA that led to DeAngelo's arrest was not analyzed using normal law enforcement forensic practices, *i.e.* by comparing it against DNA profiles already contained in CODIS. Instead, investigator Paul Holles used GEDmatch—the largest of several open-source genetic testing repositories—in a revolutionary way.[100] Founded in 2010 after DTC testing took off, GEDmatch is a service that sits downstream of the DTC companies this Article examines.[101] After for-profit DTC companies like 23andMe or Ancestry analyze a consumer's saliva sample, they send customers two things: a snapshot of their results and a computer file of raw genetic data.[102] GEDmatch allows users who have already had their DNA analyzed to upload that computer file to their website, and then compare their genome's similarity to others in GEDmatch's database.[103] Because GEDmatch is open-source, free to use, and permits aliases,[104] Holles and his team set up an "undercover profile" using the long-cold crime scene DNA on hand.[105] Their search of GEDmatch led them first to DeAngelo's ancestors, then

95. *See* Catherine W. Kimel, Note, *DNA Profiles, Computer Searches, and the Fourth Amendment*, 62 DUKE L. REV. 933, 939–40 (2013).

96. *See, e.g.*, 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 1, 1 (Oct. 2, 2018).

97. Sam Stanton & Ryan Lillis, *Relative's DNA From Genealogy Websites Cracked East Area Rapist Case, DA's Office Says*, SACRAMENTO BEE (Apr. 26, 2018, 2:01 PM), https://www.sacbee.com/news/local/crime/article209913514.html.

98. *Id.*

99. Dennis Romero & Associated Press, *Golden State Killer Suspect Arraigned On New Charges*, NBC NEWS (Aug. 23, 2018, 10:59 PM), https://www.nbcnews.com/news/crime-courts/ golden-state-killer-suspect-arraigned-new-charges-n903406.

100. Lillis, *supra* note 6.

101. *See id.*

102. 23ANDME, *Raw Genotype Data Technical Details*, https://customercare.23andme.com/hc/en-us/articles/115004459928-Raw-Genotype-Data-Technical-Details (last visited May 27, 2020)

103. *See* Lillis, *supra* note 6. In 2018 (the year police arrested DeAngelo as the Golden State Killer), GEDmatch contained genetic data from over 800,000 users.

104. *See id.*

105. *Id.*

to DeAngelo.[106] Notably, however, genetic genealogy techniques first led investigators to accuse a seventy-three-year-old man in Oregon whom they later cleared.[107]

Law enforcement's use of a new, non-CODIS genetic database generated considerable public attention and encouraged other jurisdictions and non-state actors to try similar tactics. Officers around the country have made a spate of arrests since 2018.[108] The uptick in activity seems to have also galvanized the FBI, whose future goals now include "enhance[ing] kinship analysis software . . .[and] utiliz[ing] STR and mtDNA information as well as metadata."[109] These efforts come at the same time that local police departments are investing in other DNA technologies such as Rapid DNA machines that will allow officers to analyze DNA themselves and return forensic matching data in just ninety minutes.[110] Indeed, since President Trump signed the Rapid DNA Act in 2017, police stations may be able to connect their DNA machines to directly to CODIS, making "genetic fingerprinting . . . set to become as routine as the old-fashioned kind."[111]

Private companies have embraced the opportunity to profit by linking private genetic databases with police efforts. For example, Parabon NanoLabs's "genetic genealogy" unit has, thus far, uploaded at least 100 crime scene DNA samples to GEDmatch in hopes of finding matches.[112] And, after facing backlash for disclosing its partnership with the FBI, FamilyTreeDNA has repurposed its perceived privacy defects into a new marketing technique.[113] Offering customers an opportunity to "crowd-source crime solving," FamilyTreeDNA's newest ad tells consumers they have a "moral responsibility" to stay opted in to data sharing with law enforcement and thus "prevent violent crimes, save lives, or bring closure to families."[114]

106. Cyrus Farivar, *GEDmatch, A Tiny DNA Analysis Firm, Was Key For Golden State Killer Case*, ARS TECHNICA (Apr. 27, 2018, 9:25 AM), https://arstechnica.com/tech-policy/2018/04/gedmatch-a-tiny-dna-analysis-firm-was-key-for-golden-state-killer-case/.

107. *See* Michael Balsamo et al., *Police Using Genetic Sites Misidentified Oregon Man As Golden State Serial Killer Suspect In 2017*, CHI. TRIB. (Apr. 28, 2018), https://www.chicagotribune.com/news/nationworld/ct-genealogy-site-serial-killer-20180427-story.html.

108. *See* Sarah Zhang, *Most People of European Ancestry Can Be Identified From a Relative's DNA*, THE ATLANTIC (Oct. 11, 2018), https://www.theatlantic.com/science/archive/2018/10/golden-state-killer-genealogy/572545/ (describing nineteen murderers, rapists, and unidentified persons found through open-source genetic genealogy).

109. *Combined DNA Index System (CODIS)*, FED. BUREAU INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis (last visited May 27, 2020).

110. *See* Heather Murphy, *Coming Soon to a Police Station Near You: The DNA 'Magic Box'*, N.Y. TIMES (Jan. 21, 2019), https://www.nytimes.com/2019/01/21/science/dna-crime-gene-technology.html (describing a Philadelphia suburb's debut of the Rapid DNA machine and the machine's spread to precincts in Texas, Utah, and Delaware).

111. *See id*.

112. *See* Zhang, *supra* note 91.

113. *See* Brown, *supra* note 13; *see also* FamilyTreeDNA, *Ed Smart, Father of Elizabeth Smart Teams Up With FamilyTreeDNA*, PR NEWSWIRE (Mar. 26, 2019, 3:59 PM), https://www.prnewswire.com/news-releases/ed-smart-father-of-elizabeth-smart-teams-up-with-familytreedna-300818994.html.

114. *See* FamilyTreeDNA *supra* note 113.

C. Inadequate Regulatory Oversight

Until robust regulation is enacted, nothing but the Fourth Amendment protects individuals' privacy interests in their DTC genetic testing data.

Though companies like 23andMe promise that the "guidelines we follow are essentially the same as what other research institutions follow," they do not follow such guidelines, nor are they obliged to.[115] Also, the unprecedented character of DTC genetic testing—its overlap with many fields, including medical care, research ethics, consumer protection, and criminal investigation—makes it unlikely to be regulated by any single agency or statute. DTC databases thus require privacy protections tailored specifically to the novel amalgamation of concerns they raise.

In lieu of developing an omnibus federal scheme of privacy protections, the United States "has developed a patchwork of subject specific regulations to protect the privacy of different types of information"[116] that fails to protect genetic data. This is especially true of DTC genetic testing, where different features of the tests—when regulated at all—are regulated by different or overlapping agencies.[117] Even when agencies do have some regulatory power over DTC genetic testing, overlapping authority complicates enforcement and creates opportunities to evade existing regulations.[118] Because the United States does not treat DTC genetic data as "medical" or "academic" biological data,[119] the closest DTC testing has come to robust regulation was the Food and Drug Administration's ("FDA") belated and ultimately unsuccessful attempts to curtail DTC kits' disease reporting elements.[120]

115. Megan Molteni, *23andMe's Pharma Deals Have Been the Plan All Along*, WIRED (Aug. 3, 2018, 3:28 PM), https://www.wired.com/story/23andme-glaxosmithkline-pharma-deal/.

116. PRESIDENTIAL COMM'N FOR THE STUDY OF BIOETHICAL ISSUES, PRIVACY AND PROGRESS IN WHOLE GENOME SEQUENCING 59 (Oct. 2012), https://bioethicsarchive.georgetown.edu/pcsbi/sites/default/files/PrivacyProgress508_1.pdf.

117. *See* Yuping Liu & Yvette E. Pearson, *Direct-to-Consumer Marketing of Predictive Medical Genetic Tests: Assessment of Current Practices and Policy Recommendation*s, 27 J. PUB. POL'Y. & MARKETING 131, 134 (2008). As an example, the analytic validity of genetic tests is partly governed by the Clinical Laboratories Improvement Amendments (CLIA) of 1988, which is administered by the Centers for Medicare and Medicaid Services (CMS) within the Department of Health and Human Services, whereas advertising of those tests is the purview of the Federal Trade Commission (FTC).

118. *See id*. CLIA, for instance, "ensure[s] quality laboratory testing," but is *not* responsible for mandating the "inherent safety and effectiveness" of genetic tests, or validating the claims that laboratories' make about their analytic prowess.

119. *See* Genetic Information Nondiscrimination Act of 2008, PUB. L. 110–233, 122 STAT. 881; *see also*, NAT'L HUMAN GENOME RES. INST., *The Genetic Information Nondiscrimination Act of 2008*, https://www.genome.gov/about-genomics/policy-issues/Genetic-Discrimination#gina (last visited May 27, 2020) (showing that the Genetic Information and Nondiscrimination Act clarified that genetic data could theoretically be subject to the more stringent Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule). In practice, however, GINA has had little effect. Notably, GINA does not apply to tests that look for genetic markers that are "precursors" of a disease, as DTC tests do. *See Genetic Information Privacy*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/genetic-information-privacy (last visited May 27, 2020).

120. In short, the FDA flagged 23andMe's kits as unregistered medical devices, ordered 23andMe to cease sales, was ignored, then allowed an odd détente. To sidestep subsequent FDA actions, many companies simply rebranded to focus on ancestry testing (i.e. not as "kits" that could be medical devices), yet continue to test for associations between family background and health propensities. For details, *see* PUB. HEALTH SERV., FOOD &

At the state level, regulation is similarly confused. Some states prohibit purchase of genetic tests, but in most states, "the law says nothing."[121] Utah alone has proposed legislation that would require police to obtain a court order or warrant before accessing private genetic data stored with third parties, such as DTC companies.[122] Even that legislation, however, has yet to be signed into law and contains potential loopholes for "emergency situations" and data that might be "involved" in committing certain felonies or misdemeanors.[123]

These "regulatory deficits" have been noticed and ignored by lawmakers.[124] Several large-scale studies have recommended enacting a federal regulatory scheme tailored to genetic testing, including the 1995 National Institutes of Health Task Force on Genetic Testing and the 2000 Secretary's Advisory Council on Genetic Testing.[125] But, "policy makers, including legislators, are either unsure of how to proceed or unwilling to create and enforce much needed regulations."[126] In the face of uncertain common law contours, it is thus crucial that we understand how, and to what extent, the Fourth Amendment protects DTC genetic data.

III. THE AMBIGUOUS SCOPE OF "THIRD-PARTY DOCTRINE"

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[127] It aims to balance an individual's right to privacy against the government's interest in conducting law enforcement investigations.[128] Per the Amendment, a police search of things within the four enumerated categories is presumptively unreasonable absent a warrant, unless the government can state a valid exception to the warrant requirement.[129]

Under the "third-party doctrine," individuals have no reasonable expectation of privacy in information an individual voluntarily shared with a third party.[130] Thus, Fourth Amendment protections do not apply, and government collection of such records is not a search requiring a warrant. In the context of

DRUG ADMIN., WARNING LETTER TO 23ANDME, INC. (Nov. 22, 2013); Katherine Drabiak, *Caveat Emptor: How the Intersection of Big Data and Consumer Genomics Exponentially Increases Information Privacy Risks*, 27 HEALTH MATRIX 143, 151–52 (2017); Anna Vlastis, *How 23andMe Won Back The Right To Foretell Your Diseases*, WIRED (Apr. 8, 2017, 7:00 AM), https://www.wired.com/2017/04/23andme-won-back-right-foretell-diseases/; Jennifer K. Wagner, *The Sky Is Falling for Personal Genomics! Oh, Nevermind. It's Just a Cease & Desist Letter from the FDA to 23andMe.*, PRIVACY REP. (Dec. 3, 2013), https://theprivacyreport.com/2013/12/03/the-sky-is-falling-for-personal-genomics-oh-nevermind-its-just-a-cease-desist-letter-from-the-fda-to-23andme/.

121. Liu & Pearson, *supra* note 117.

122. *See* Electronic Information or Data Privacy Act, H.B. 57, 2019 Gen. Sess. (Utah 2019).

123. *See id*.

124. *See* Liu & Pearson, *supra* note 117, at 134.

125. *Id.*

126. *See id*.

127. U.S. CONST. amend. IV.

128. Orin S. Kerr, *The Effect of Legislation on Fourth Amendment Protection*, 115 MICH. L. REV. 1117, 1123 (2017).

129. *Id.* at 1123–24.

130. Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018).

DTC genetic testing, the government might justify a warrantless search of DTC databases on the grounds that customers have voluntarily shared their genetic data with the company and other users searching for genealogical connections. In *Carpenter*, the Supreme Court's most recent third-party doctrine case, Justice Gorsuch anticipated that the Court might soon have to address the doctrine's potential application to police searches of genealogical databases.[131]

Part III traces the evolution of the third-party doctrine, from its origins through to the Court's decision in *Carpenter*.[132] Though third-party doctrine originated in case law intended to increase Fourth Amendment protections, paradoxically subsequent cases applying the doctrine eroded them.[133] Many of the Court's third-party doctrine holdings suggest unsatisfying and absurd results, illustrating that current conceptions of the doctrine are not equipped to handle rapid gains in surveillance technology capabilities, including those related to DTC genetic testing.[134]

A. The Origins of Third-Party Doctrine

Third-party doctrine, to the extent it exists as a coherent rule, has never immunized all information that is knowingly shared with others from Fourth Amendment protection. Rather, it emerged from the "reasonable expectation of privacy" test in *Katz*, which was intended to expand, not limit, Fourth Amendment protection to non-physical searches of sensitive information.[135] Problematically though, *Katz* used non-sensitive information freely shared with others as its point of comparison.[136] And, in subsequent cases, the Court failed to explain the effect an increasingly digitized society has on which expectations of privacy are legitimate, inadvertently creating a broad rule that largely eviscerated Fourth Amendment protections whenever data is shared willingly with others.[137]

Now, as information is gathered in greater quantities and kinds than ever before, the line between sensitive and non-sensitive information is even fuzzier. In 2018, the Court in *Carpenter* correctly reined in the third-party doctrine but did so in a poorly reasoned manner.[138] Accordingly, the Court offered little clarity as to the third-party doctrine's applicability to both DTC genetic testing databases and other databases involving information generated (at least partly) by third parties after being shared by individuals.[139]

For much of its existence, Fourth Amendment search doctrine centered on physical trespass. Following ratification in 1791, the Fourth Amendment remained largely unexamined by courts until a series of Prohibition-era cases

131. *See infra* Part III.C (discussing Gorsuch dissent in *Carpenter*, 138 S. Ct. at 2262–63).

132. *Carpenter*, 138 S. Ct. at 2210.

133. *See infra* Part III.B.

134. *See infra* Part IV.

135. *See* Timothy C. MacDonnell, *The Rhetoric of the Fourth Amendment: Toward a More Persuasive Fourth Amendment*, 73 WASH. & LEE L. REV. 1869, 1900–01 (2016).

136. *See* Katz v. United States, 389 U.S. 347, 351–53 (1967).

137. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2271–73.

138. *See generally id.*

139. *See id.* at 2223.

opened a rich vein of discussion over whether a Fourth Amendment "search" was limited to instances of physical trespasses.[140] In *Olmstead v. United States*, wiretapping evidence against a rumrunner was found admissible because the police's installation of the device did not involve a physical trespass into the defendant's home.[141] Writing for a majority of five, Chief Justice Taft emphasized that a Fourth Amendment "search is to be of material things—the person, the house, his papers or his effects."[142] Taft harkened back to the historical target of the Fourth Amendment, which was to prevent "misuse of governmental power of compulsion"[143] in the manner that the British had through use of general warrants and writs of assistance.

In response, Justice Brandeis's vociferous dissent accused the majority of following the letter of the Fourth Amendment at the expense of its spirit. The dissent recognized a fundamental "right to privacy"[144] and suggested that this right included a comprehensive and valuable "right to be let alone."[145] Brandeis's chief and prescient worry was that as "time works changes,"[146] "the progress of science in furnishing the Government with means of espionage"[147] would encourage progressive encroachment upon Fourth Amendment protections.[148] According to Brandeis, the chief offense of warrantless searches was their element of government "compulsion."[149] For that reason, Fourth Amendment rights, "would not be violated, under any ordinary construction of language, by compelling obedience to a subpoena."[150]

Significantly influenced by Brandeis's dissent, the majority in *Katz* rejected the physical trespass test because it artificially restricted the scope of Fourth Amendment protections.[151] *Katz* overruled *Olmstead* by 7-1, and forcefully held that "the Fourth Amendment protects people, not places."[152] In deciding that the police's eavesdropping on Katz from outside the telephone booth was a Fourth Amendment violation, *Katz* expanded the Fourth Amendment's protections beyond tangible physical trespasses to intrusions into any space where individuals have a "reasonable expectation of privacy" in the information sought.[153] Writing for the majority, Justice Stewart explicitly referred to a concept of personal pri-

140. *See infra* text accompanying notes 141–56.

141. Olmstead v. United States, 277 U.S. 438 (1928).

142. *Id*. at 464.

143. *Id.* at 463. The quoted phrase ("misuse of governmental power of compulsion") was actually the focus of four major Fourth Amendment cases: Boyd v. United States, 116 U.S. 616 (1886); Weeks v. United States, 232 U.S. 383 (1914); Silverthorne Lumber Co. v. United States, 251 U.S. 385 (1920); and Amos v. United States, 255 U.S. 313 (1921).

144. *Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting).

145. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195–96 (1890).

146. *Olmstead*, 277 U.S. at 472 (Brandeis, J., dissenting).

147. *Id.* at 474.

148. *Id*.

149. *Id.* at 477.

150. *Id.* at 476.

151. Katz v. United States, 389 U.S. 347, 353 (1967).

152. *Id.* at 351.

153. *See id*. at 357–58.

vacy that extended beyond personal property or nonpublic spaces: "[W]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. *But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.*"[154] In this way, *Katz* reframed the test for determining a search from physical trespass to the existence of a "reasonable expectation of privacy."[155] It would go on to become third-party doctrine's founding case. In addition, the *Katz* Court said, "'Over and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes,' and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable."[156]

As *Katz* did not clarify its relationship to search doctrine's roots in property law[157] or how a court could determine if society held a particular "reasonable expectation of privacy,"[158] search doctrine developed along two distinct paths, both of which misinterpret *Katz*. The first path "appears to remove property law from the Fourth Amendment."[159] The other has not.[160] Arguably, the latter leads courts squarely back to a physical trespass test, which ignores the impetus behind *Katz*, while the former defines a "legitimate expectation of privacy" based almost solely upon whether or not third parties have the information at issue.[161]

This latter path is particularly problematic for reasons explored (though not named) by the Court in *Carpenter*. It, however, is the strand of search doctrine that has contributed most to the Court's creation of third-party doctrine.[162] It is therefore important to examine two cases that came after *Katz*: *United States v. Miller* (1976) and *Smith v. Maryland* (1979).[163] Both *Miller* and *Smith* applied *Katz* incorrectly, and in doing so elaborated upon its "reasonable expectation of privacy" test in ways that created additional confusion.[164]

154. *Id.* (emphasis added) (citation omitted).

155. United States v. Jones, 565 U.S. 400, 405–06 (2012).

156. *Katz*, 389 U.S. at 357 (quoting United States v. Jeffers, 342 U.S. 48, 51 (1951)).

157. *See e.g*. Soldal v. Cook County, 506 U.S. 56, 64 (1992) (clarifying that the "message" of *Katz* and its following cases "is that property rights are not the sole measure of Fourth Amendment violations.").

158. How to reliably determine society's views on privacy engenders significant debate. Recently, a number of empirical studies and surveys have attempted to shed light on the question. *See e.g.*, Bernard Chao, Catherine Durso, Ian Farrell & Christopher Robertson, *Why Courts Fail to Protect Privacy: Race, Age, Bias, and Technology*, 106 CALIF. L. REV. 263 (2018) (conducting a large scale survey of 1,200 people and finding that expectations of privacy varied depending on which of the eighteen selected police practices was at issue and that courts generally underestimated how intrusive the public felt those practices were); Matthew B. Kugler & Lior J. Strahilevitz, *The Myth of Fourth Amendment Circularity*, 84 U. CHI. L. REV. 1747 (2017) (conducting surveys on census weighted samples of US citizens immediately before, immediately after, and long after the Supreme Court's decision in *Riley v California*, and finding that popular privacy expectations are far more stable than most judges and commentators have assumed).

159. *See* Timothy C. MacDonnell, *The Rhetoric of the Fourth Amendment: Toward a More Persuasive Fourth Amendment*, 73 WASH. & LEE L. REV. 1869, 1901 (2016).

160. *Id.* at 1897–98.

161. *See id.* at 1895–1909.

162. *See* Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018); Chao et al., *supra* note 158, at 302.

163. *See infra* pages 1273–76.

164. *See infra* pages 1273–76.

In *Miller*, the Court dramatically expanded third-party doctrine by holding that individuals have no reasonable expectation of privacy in documents they provide to their bank, because "all of the documents. . . contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[165] But in order to conclude that banks were "public" for purposes of search doctrine, the Court ignored the language from *Katz* that declared "what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[166] Instead, the Court leaned on the Bank Secrecy Act, which required banks to maintain records because of their "high degree of usefulness in criminal, tax, and regulatory investigations and proceedings."[167] The Act, though not part of traditional Fourth Amendment case law, was likely why the Court assumed public notice of possible law enforcement surveillance and placed the burden on the defendant for safeguarding his own financial privacy.[168] Thus, in the same breath that the Court acknowledged that the defendant wanted to keep his financial information private, and in a broader sense, treated it as private except in sharing it with the one entity he had to (*e.g.* the bank), the Court also advanced a view of privacy akin to a Pandora's box: once opened to a "third-party," it cannot be cloistered again.

The Court in *Smith* stretched *Miller*'s sweeping language even further. In *Smith*, the Court held that there was no expectation of privacy in the records of dialed telephone numbers conveyed to a telephone company, because the phone company automatically received the numbers when dialed.[169] As justification, the Court declared that it "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[170] In this way, the Court completely overlooked the need to distinguish between "public" and private third parties that *Miller* skirted. Moreover, it did so by ignoring significant distinctions between the five cases it cited as support.[171] The cases relied upon all involved situations in which a clearly "public" entity, *i.e.*, the government, was already involved.[172] First, the Court in *Couch*, though it devoted less than a paragraph to discussion of the Fourth Amendment, emphasized that tax accountants, presumably like banks, are required to share the information they are entrusted with.[173] Moreover, the Court assumed that all parties were aware that, by law, "the accountant himself risks criminal prosecution

165. United States v. Miller, 425 U.S. 435, 442 (1976).

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

167. *Miller,* 425 U.S. at 442–43 (quoting 12 U.S.C. § 1829b (a)(1) (1976)).

168. *Id*. at 443 (stating that a "depositor takes the risk" that once he has "reveal[ed] his affairs to another," that the information could end up in Government hands).

169. Smith v. Maryland, 442 U. S. 735, 744–46 (1979).

170. *Id*. at 743–44.

171. *Id*. (citing *Miller*, 425 U.S. at 442–44; Couch v. United States, 409 U.S. 322, 335–36 (1973); United States v. White, 401 U.S. 745, 752 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427 (1963)).

172. *See supra* note 167 and accompanying text; *infra* notes 173–77 and accompanying text.

173. *Couch*, 409 U.S. at 335 (finding "little expectation of privacy where records are handed to an accountant, knowing that mandatory disclosure of much of the information therein is required in an income tax return").

if he willfully assists in the preparation of a false return."[174] Likewise, in *White*, *Hoffa*, and *Lopez*, the Court held that, "however strongly"[175] a defendant trusts his colleagues, if that colleague is a government agent[176] operating within the scope of employment, breach of even a legitimate expectation of privacy is constitutionally "justifiable."[177] Despite their differences, however, the *Smith* Court drew on these five cases to assume that "all telephone users realize that they must 'convey' phone numbers to the telephone company,"[178] even if they "harbor[ed] some subjective expectation" of privacy.[179] As in *Miller*, *Smith* thus announced its holding without explaining how it reached it, and in doing so, again subverted *Katz*'s protective aims by expanding the records police could access *sans* warrant.[180]

Commentators have referred to the Court's interpretation of Fourth Amendment rights in *Katz*, *Miller*, and *Smith* as the "third-party doctrine."[181] Generally, the doctrine is this: by voluntarily giving information to *any* third party, an individual forsakes his or her reasonable expectation of privacy in that data.[182] Fourth Amendment protections do not apply, and what might otherwise be a "search" requiring a warrant under the Fourth Amendment no longer is.[183]

The expansive third-party "doctrine" that existed by the end of the 1970s eviscerated Fourth Amendment protections whenever an individual shared their information with any third party that was not privileged. And indeed, the results of such cases seem odd: in *Miller* and *Smith*, for instance, the records at issue (bank records and phone numbers dialed, respectively) contained personal and sensitive information; it was seemingly the defendant's mere act of sharing that information with another that rendered it unprotected.

Yet, *Smith* and *Miller*, even as they ostensibly created a broad implicit third-party doctrine, relied on particular facts that could leave room for protection of more sensitive or intrusively accessed data, even if shared with others. First, *Smith* noted that the police were accessing only metadata, not content.[184] Second, the Court has suggested that less sophisticated technologies were less concerning, because they disclosed only rudimentary personal information.[185] In *Miller*, the Court emphasized that pen registers used by police to obtain information were "limited" in their surveillance capabilities and police could not "determine from the use of a pen register whether a communication existed."[186]

174. *Id.* (quoting 26 U.S.C. § 7206 (2) (1970)).
175. *White*, 401 U.S. at 749.
176. In *Lopez*, an internal revenue agent, and in *White* and *Hoffa*, a paid informant. *See White*, 401 U.S. at 746–47; *Hoffa*, 385 U.S. at 296; *Lopez*, 373 U.S. at 428.
177. *See White*, 401 U.S. at 751–52.
178. *Smith*, 442 U.S. at 742.
179. *Id.* at 743.
180. *See generally id.*
181. *See, e.g.*, Chao et al., *supra* note 158, at 271.
182. *See id*.
183. *Id*. at 271–72.
184. *Smith*, 442 U.S. at 741–42.
185. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2215–18 (2018).
186. *Smith*, 442 U.S. at 741, 742.

But the Court has offered little guidance on when, how, or why a court (as opposed to legislatures) can decide if a technology's surveillance capability is "limited."[187] Moreover, what if, as in *Miller* rather than *Smith*, the information's contents *are* accessed? What kinds of contents are protected? It quickly becomes untenable to continue using third-party doctrine, given that the Court has never explained how to determine what expectations of privacy are "reasonable."[188] Legal scholars have called this chicken-egg conundrum of privacy expectations, "the circularity problem."[189] As then-Professor Richard Posner summarized, "it is circular to say that there is no invasion of privacy unless the individual whose privacy is invaded had a reasonable expectation of privacy; whether he will or will not have such an expectation will depend on what the legal rule is." [190]

B. Inconsistent Doctrinal Development: A Return to Property Law Jurisprudence in Jones

Faced with the difficulty of consistently applying third-party doctrine, in 2012 the Court in *Jones v. United States* appeared to take refuge in the Fourth Amendment's property law roots. *Jones*, however, addressed none of the issues *Miller* and *Smith* raised, and muddied the waters of third-party doctrine by applying the physical trespass test from *Olmstead* without incorporating *Katz*.[191]

In *Jones*, police physically placed a GPS tracker on the undercarriage of Jones's car without a valid warrant, and then monitored its movements for twenty-eight days.[192] The Court held that, per physical trespass, the Government conducted a search and violated Jones's Fourth Amendment rights.[193] In so holding, the Court implied that *Katz*'s "reasonable expectation of privacy" test did not entirely invalidate pre-*Katz* cases relying on tangible intrusions.[194]

The *Jones* majority relied upon trespass theory in part because such reasoning justified postponing "thorny problems" of whether the government's prolonged digital surveillance of Jones violated a "reasonable expectation of privacy"[195]—*i.e.*, how *Katz* operates in a digital era. This evasion led Justice Sotomayor to announce in her oft-cited concurrence that third-party doctrine imminently needed revision because "the same technological advances that have made possible non-trespassory surveillance techniques will also affect the *Katz* test by shaping the evolution of societal privacy expectations."[196] After all, so-

187. *Id.*

188. United States v. Miller, 425 U.S. 435, 442 (1976).

189. *See, e.g.,* Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 SUP. CT. REV. 173, 188, n.41.

190. *Id.*

191. *See Jones*, 565 U.S. at 405–08.

192. *See id.* at 402–03.

193. *Id*. at 407–08.

194. *Id.*

195. *See id.* at 412.

196. *Id.* at 415, 417 (Sotomayor, J., concurring) (questioning whether it may be "necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to

cietal privacy expectations are increasingly difficult to determine as sophisticated technologies (and, as Part IV will explain, DTC genetic testing in particular) force people to be subject to ongoing surveillance without their informed consent.[197]

C. Carpenter*, The Current State of Third-Party Doctrine, and Continuing Confusion*

In light of the issues raised by the cases that built upon *Katz* and the Court's return to property law in *Jones*, the *Carpenter* case heralded an opportunity to explicitly name, clarify, and update the third-party doctrine so that it might reflect modern technologies and understanding of information gathering and usage. In a seeming win for privacy, *Carpenter* held that individuals have a reasonable expectation of privacy in their cell-site location information; therefore third-party doctrine does not apply.[198] Yet, the Court again reached its holding in a manner that neither addressed pre-existing doctrinal confusions nor enabled the doctrine to be consistently applied going forwards.[199]

Carpenter involved a challenge to a warrantless search of cell site location information ("CSLI"), teeing up the Fourth Amendment's post-*Katz* application (or not) to highly sensitive records that a suspect had technically shared with a third party. Specifically, law enforcement obtained cell-site location information from Carpenter's wireless carriers and used that so-called metadata to map his whereabouts during and after a string of robberies.[200] Because cell phones continuously scan for the best signal by continuously pinging nearby cell sites (even when the phone's owner is not actively using the phone) and most people "compulsively carry cell phones with them all the time,"[201] the police gleaned data that painted an intimate hour-by-hour portrait of Carpenter's movements over the course of 127 days.[202]

As troubled as Justice Brandeis had been a century earlier that advancing technology[203] would corrode Fourth Amendment rights, a majority of the Court held that law enforcement committed an unconstitutional search because "individuals have a reasonable expectation of privacy in the whole of their physical movements."[204] In this way, the Court properly limited the seemingly limitless reach of third-party doctrine in an era when individuals routinely can, and often must, give their information to third parties.[205]

---

third parties. . . [in] the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks").

197. *See* discussion *infra* Part IV.A.1.

198. *See* Carpenter v. United States, 138 S. Ct. 2206, 2219, 2223 (2018).

199. *Id.*

200. *Id.* at 2212.

201. *Id.* at 2211, 2218.

202. *Id.* at 2212.

203. *Id*. at 2223 (quoting Olmstead v. United States, 277 U. S. 438, 473–74 (1928) (Brandeis, J., dissenting)).

204. *Id.* at 2217 (citing United States v. Jones, 565 U.S. 400, 430, 415 (2012) (concurring opinions of Justices Alito and Sotomayor)).

205. *See id.* at 2216–19.

But in its attempt to create a narrow exception to the third-party doctrine, the *Carpenter* Court overstated the "unique" nature of the technology at issue, and glossed over why that technology was entitled to Fourth Amendment protection.[206] This maintained pre-existing confusions raised by *Katz* and its subsequent cases, and *Jones*; and raised three additional concerns.

First, though *Carpenter*'s use of "expectation of privacy" language pays tribute to the *Katz* test, the Court focused its reasoning on three novel factors that do not cleanly overlap with the core premises of third-party doctrine in *Katz*, *Smith*, and *Miller*: that there is a reduced expectation of privacy in one's "public movements"[207] and in information voluntarily exposed to third parties.[208] The three novel factors are: "the deeply revealing nature of [cell phone location metadata]"; "its depth, breadth, and comprehensive reach;" and "the inescapable and automatic nature of its collection."[209] The Court held that because these factors applied to CSLI data, the fact the information was possessed by a third party did not exempt it from Fourth Amendment protection.[210] The Court did not state whether the existence of the three factors in a particular context make the act of sharing information with a third party "public" (and therefore exempt from the Fourth Amendment) or how the factors should be weighed.[211] Moreover, the factors do not address *why* CSLI data is "deeply revealing" compared to other surveillance technologies and thus avoid addressing what underlies the Court's third-party cases generally.[212]

Second, though the Court applied the *Katz* test and then appeared to reformulate it, the majority insisted it has "kept this attention to Founding-era understandings" of the Fourth Amendment's roots in property law.[213] This perpetuates the confusion caused by *Jones* as to the relative importance of the property-law based trespass test and the Court's newer, less tangible tests such as *Katz* and *Carpenter*.[214] Third, in emphasizing that it views cell-site records as a "qualitatively different category" of data,[215] the majority ignored that cell-site data is not, in fact, a "seismic shift,"[216] but rather, part of a larger trajectory of digital technologies towards big data, of which genetic testing is also part.

Interestingly, because both the majority and Justice Gorsuch's dissent agreed that the Framers were determined "to place obstacles in the way of a too permeating police surveillance" into "the privacies of life,"[217] there may be a way forward from *Carpenter* that does justice to the purpose of the Fourth

206. *See id.* at 2217.
207. *Id.* at 2219–20.
208. *Id.*
209. *Id*. at 2223.
210. *Carpenter*, 138 S. Ct. at 2206, 2223.
211. *See id.*
212. *See id.*
213. *Id*. at 2214.
214. *See Carpenter*, 138 S. Ct. at 2213; *Jones*, 565 U.S. at 411; *Katz*, 389 U.S. at 353.
215. *Carpenter*, 138 S. Ct. at 2216–17.
216. *Id.* at 2219.
217. *Id.* at 2214 (quoting United States v. Di Re, 332 U.S. 581, 595 (1948) and Boyd v. United States, 116 U. S. 616, 630 (1886)).

Amendment by looking backwards to the Court's property-based search doctrine jurisprudence before *Katz*.[218] To this end, Justice Gorsuch's dissent reads more like a concurrence, given that he ultimately agreed that the seizure of the cell location records violated the Fourth Amendment.[219] Justice Gorsuch suggested that Carpenter might have an "ancient"[220] property interest in the contents of his cell phone data, though he did not elaborate because Carpenter did not argue this in the lower courts.[221] Such a view would likely require updating common law property doctrines to reflect what comes under the Fourth Amendment's protected categories of "persons. . . and effects," but, as the next Part will argue, perhaps would more effectively prevent the government's warrantless access to sensitive modern data troves such as DTC DNA databases.[222]

In his dissent, Justice Gorsuch mentioned 23andMe by name, marveling that the third-party doctrine appears to allow the police to access its records according to "*Smith* and *Miller*. . . without running afoul of *Katz*" though "that result strikes most lawyers and judges today—me included—as pretty unlikely."[223] While this what-is-old-is-new reading of the Fourth Amendment raises issues regarding what would constitute a property interest,[224] the majority opinion together with Justice Gorsuch's dissent may in time see *Carpenter* open up a robust view of the Fourth Amendment. Such a view could be once again grounded in pre-*Katz* property law but updated to reflect what modern society feels it has ownership interests in. After all, *Katz*'s reasonable expectation of privacy test was an effort to expand Fourth Amendment protections at a time when wireless advances rendered the traditional property rules ineffective. Now, arguably, a second, Big Data-based revolution has flipped that script so that a property rule might again become the more protective path.[225]

IV. A PATH FORWARD: WHY THIRD-PARTY DOCTRINE DOES NOT, AND SHOULD NOT, APPLY TO DTC DNA DATABASES

No formulation of the third-party doctrine applies well to DTC genetic testing data, nor should it. And, at any rate, *Carpenter*'s emphasis on the narrowness of its holding leaves third-party doctrine's application to DTC DNA databases an unresolved question.[226]

218. *See Carpenter*, 138 S. Ct. at 2267–68 (Gorsuch, J., dissenting).
219. *Id.* at 2272.
220. *Id.* at 2269.
221. *Id.*
222. *Id.* at 2268–69.
223. *Id*. at 2262.
224. *See generally* Pamela Samuelson, *Privacy As Intellectual Property?* 52 STAN. L. REV. 1125 (2000).
225. *See Carpenter,* 138 S. Ct. at 2227.
226. *See id.*, at 2210 ("This decision is narrow. It does not express a view on matters not before the Court; does not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras; does not address other business records that might incidentally reveal location information; and does not consider other collection techniques involving foreign affairs or national security").

As Part IV explains, *Carpenter* fails to protect DTC genetic data from warrantless government collection enabled by the third-party doctrine.[227] This is troubling because the personal information at issue is hypersensitive and DTC companies have financial incentives to work with law enforcement, even at the possible expense of their customers' liberties.[228] Accordingly, the Court should look to the historical purpose of the Fourth Amendment and a major theme underlying search doctrine jurisprudence: namely, that fulfillment of a warrant requirement provides Fourth Amendment protections to private citizens and allows law enforcement to conduct targeted searches based on good evidence.

A. Why Get a Warrant?

On its face, the Fourth Amendment does not prohibit the government from accessing all forms of private information.[229] It's protections are for the individual's right to be "secure . . . against *unreasonable* searches and seizures."[230] Historically, what made police actions unreasonable was largely a question of whether or not officials adhered to proper criminal procedure during investigations.[231]

In lieu of protective regulatory oversight, requiring police to obtain a warrant or court order introduces critical limitations on police access to personal information that it might or should not have.[232] Warrants require a number of specific criteria to be met before police may search the people or places requested, and they must be signed by a judge or magistrate.[233] Here, the judge's presence would be an important bulwark against freewheeling genetic database searches by police because, ideally, a judge would not grant a warrant that did not cabin the section of the genetic database to be searched and would ensure it list specific traits or targets being searched for.[234] Moreover, just the process of getting a warrant helps create a hard record that promotes accountability and might diminish public fears of vast searches conducted in secret by police.

More importantly, warrants diminish the likelihood that the government can conduct "data dumps" that unduly expand existing forensic databases, or that

227. *See infra* Part IV.C.

228. *See infra* Part II.A.

229. U.S. CONST. amend. IV.

230. *See id.* (emphasis added).

231. *See, e.g.*, ERWIN CHEMERINSKY & LAURIE L. LEVENSON, CRIMINAL PROCEDURE ADJUDICATION 15–16 (3d ed. 2008).

232. *See, e.g.* WAYNE R. LAFAVE ET AL., SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT 441–46 (4th ed. 2004).

233. Critically, a warrant for genetic data should be specific to a type of genetic insight and particular crime under investigation. *See e.g.* Tony Webster, *Minnesota judge signs a search warrant for personal information on anyone who Googled someone's name*, TONY WEBSTER, https://tonywebster.com/2017/03/minnesota-search-warrant-anyone-who-googled/ (last visited May 27, 2020).

234. In other words, a judge should *not* grant a warrant like the one recently obtained in Florida, which allowed a detective to penetrate GEDmatch and search its full database of nearly one million users *despite* the company's choice to restrict police access to its records as of early 2019. *See* Kashmir Hill and Heather Murphy, *Your DNA Profile is Private? A Florida Judge Just Said Otherwise*, N.Y. TIMES (Nov. 5, 2019), https://www.nytimes.com/2019/11/05/business/dna-database-search-warrant.html (last updated Dec. 30, 2019).

DNA data will be used for impermissible reasons (*i.e.* for purposes other than suspect identification).[235] To obtain a warrant, officers must demonstrate probable cause justifies their search, and crucially, must specify in writing the place they will search, the items they will seize, and depending on the judge's discretion, how and when police will conduct the search.[236] Thus, warrants could prevent law enforcement from indiscriminately combing through thousands of customers' genetic information and enable targeted searches based on evidence that is likely to remain admissible at trial.

This extra scrutiny could allay public concerns that law enforcement may obtain genetic information—for example, on ethnic origin and appearance—for identification purposes, but then keep or exploit that data in impermissibly discriminatory ways. Notably, CODIS, the existing forensic database used by local, state, and federal law enforcement agencies, already overrepresents certain vulnerable communities, and some have argued that familial DNA testing in particular might further result in disproportionately greater surveillance of vulnerable groups.[237] Such safeguards against "arbitrary use of state violence" are vital in order to maintain individuals' Fourth Amendment right to privacy, sense of "peoplehood," and the space to dissent that democracy requires.[238]

1. DNA as Destiny: The Dangers of Policing with Genetic Data

History warns us against allowing unlimited government access and storage of individuals' DNA without exercising rigorous caution and public accountability.[239] For decades, if not centuries, researchers have studied whether hereditary or genetic components might determine or raise the risk of criminal conduct.[240] In *Buck v. Bell*, for example, the infamous case in which the Supreme Court upheld Carrie Buck's forced sterilization, the Court explicitly drew a connection between genetics and crime: "It is better for all the world, if instead of waiting to execute degenerate offspring for crime. . . society can prevent those who are manifestly unfit from continuing their kind. . . Three generations of imbeciles are enough."[241] Though *Buck* has been rightly castigated in years since, its belief in an inheritable criminal taint risks resurfacing as investigative genealogy gains traction.[242] At any rate, *Buck* serves as a poignant warning of the

235. *Id.*

236. *Id.*

237. *See generally* Daniel J. Grimm, Note, *The Demographics Of Genetic Surveillance: Familial DNA Testing and the Hispanic Community*, 107 COLUM. L. REV. 1164 (2007) (arguing that familial DNA testing will disproportionately affect the Hispanic community, in part because of their tendency to have large families).

238. ANDREW E. TASLITZ, RECONSTRUCTING THE FOURTH AMENDMENT: A HISTORY OF SEARCH AND SEIZURE, 1789–1868 65 (2006).

239. Susan Scutti, *The Government Owns Your DNA. What Are They Doing with It?*, NEWSWEEK (July 24, 2014, 3:50 PM), https://www.newsweek.com/2014/08/01/whos-keeping-your-data-safe-dna-banks-261136.html.

240. *See generally* Mark A. Rothstein, *Applications of Behavioural Genetics: Outpacing the Science?*, 6 NATURE REVS.: GENETICS 793 (2005).

241. *See* Buck v. Bell, 274 U.S. 200, 207 (1927).

242. *Cf.* Jamal Greene, *The Anticanon*, 125 Harv. L. Rev. 380, 382 (2011) (cautioning scholars constructing arguments featuring "anticanonical" cases such as Dred Scott v. Sandford and Korematsu v. United States).

"extent to which developing science was seized upon and used by nonscientists—policymakers, politicians, judges, and lawyers—who sought to dress their agendas in the trappings of legitimate scientific debate"[243] and lends weight to historically recurrent fears that novel research findings or technologies will be used in oppressive and reactionary ways.[244]

Using genetics to scavenge for associations between genotypes and criminal behavior remains a popular avenue of study.[245] In fact, recent years have seen increasing "interest and demand for scientific explanations about human behavior."[246] Between 1994 and June of 2007, "at least 48 criminal cases relied on behavioral genetics evidence in a wide range of ways."[247]

While behavioral genetics cannot provide conclusive evidence of guilt or innocence, Professor Henry Greely has noted, "if the behavior cannot necessarily be observed in a suspect because it is only a propensity—an increased likelihood of acting in a particular way—rather than an invariant behavior, genomic analysis might indeed show whether a person had that higher likelihood."[248] For example, some studies claim that a lack of a functional *MAO-A* gene in males is correlated with a high likelihood of committing arson at some point, and could help police identify and arrest arson suspects.[249] That even rudimentary behavioral genetics data can be used by law enforcement, despite likely being inadmissible at trial due to unsound science, is troubling and suggests that other parts of the criminal process might likewise lean on questionable genetic insights. The rising use of risk assessments based on neuroscience in settings such as criminal sentencing provides one example.[250] Thus, such assessments leave the door open to drawing future associations between traits tested by DTC companies, such as particular ancestry, with criminal conduct such as recidivism.

243. Owen D. Jones, *Behavioral Genetics and Crime, in Context*, in THE IMPACT OF BEHAVIORAL SCIENCES ON CRIMINAL LAW 157 (Nita A. Farahany, ed., 2009).

244. *See id.* at 156 n.38 (describing how nineteenth-century Italian physician Cesare Lombroso first proposed the idea of the "born" criminal, a theory that–despite being disproven–played a significant role in the American eugenics movement a century later and continues to influence social understandings of criminality today).

245. *See, e.g.* John Pyun, *When Neurogenetics Hurts: Examining the Use of Neuroscience and Genetic Evidence in Sentencing Decisions Through Implicit Bias*, 103 CALIF. L. REV. 1019, 1019 (2015); Rothstein, *supra* note 240; Gregory L. Stuart et al., *Further Investigation of Genetics and Intimate Partner Violence*, 20(4) VIOLENCE AGAINST WOMEN 420, 420 (2014); J. Tiihonen et al., 20 *Genetic Background Of Extremely Violent Behavior*, MOLECULAR PSYCHIATRY 786, 786 (2015).

246. Nita A. Farahany, *Introduction* to THE IMPACT OF BEHAVIORAL SCIENCES ON CRIMINAL LAW at xi (Nita A. Farahany, ed., 2009).

247. Deborah W. Denno, *Behavioral Genetics Evidence in Criminal Cases: 1994-2007*, *in* THE IMPACT OF BEHAVIORAL SCIENCES ON CRIMINAL LAW 317, 321 (Nita A. Farahany, ed., 2009).

248. *See* Greely, *supra* note 14, at 172–73.

249. *Id*. at 173.

250. These actuarial assessments do not ask why variables are correlated with criminal conduct—arguably, they just use them. *See* Jeremy Isard, *Under the Cloak of Brain Science: Risk Assessments, Parole, and the Powerful Guise of Objectivity*, 105 CALIF. L. REV. 1223, 1241–54 (2017) (describing how psychological risk assessment tools used by the California Board of Parole Hearings have a "distinct ability to reframe historical, immutable, and demographic variables as contemporaneous risk factors . . . ."); Sonja B. Starr, *Evidence-Based Sentencing and the Scientific Rationalization of Discrimination*, 66 STAN. L. REV. 803, 806 (2014) (arguing that the growing trend of basing criminal sentences on actuarial risk predictions that include demographic and socioeconomic variables violates the Equal Protection Clause).

Once law enforcement has access to an individual's DNA sample, there appears to be no limit on the number of times that sample can be reanalyzed; in this way, law enforcement can mine DNA samples for insights not available at the time they were obtained. This is a form of function creep that courts must guard against. For example, CODIS, the existing national DNA database, prompts reanalysis of an individual's DNA sample every time it appears as a CODIS search hit.[251] There seems to be no limit whatsoever on retesting genetic samples obtained from DTC companies.

There is no telling what repeated future testing might foretell for any putative suspect targeted by the government. Though new genetic association studies are regularly published, like quicksand, "consensus on what different genetic variations mean for disease risks changes over time, as new information comes in."[252] One analysis found that "from 2016 through 2017, more than 7,500 mutations were reclassified, most of them from 'pathogenic' or 'likely pathogenic' to 'unknown' or 'conflicting significance.'"[253] The fact that "DNA samples that are on file could be reanalyzed at more informative sites, and statistical studies of possible correlations between the new data and behavioral traits" thus amplifies fears that cross-pollination between police and DTC databases may be used improperly.[254]

Because investigative techniques based on DNA data are susceptible to errors, a court order or warrant requirement cannot guarantee that police searches will be accurate. It does, however, add a constitutional checkpoint to the criminal process. The increasingly fine scale at which DNA technologies now operate is a significant culprit. "It's now possible to detect DNA at levels hundreds or even thousands of times lower than when DNA fingerprinting was developed in the 1980s . . . A mere 25 or 30 cells will sometimes suffice."[255] Numerous cases, including that of Amanda Knox, who was accused of murdering her housemate during a year abroad in Italy, demonstrate that "heightened sensitivity can easily create false positives."[256] Indeed, the accuracy of DTC genetic tests is cause for concern. For example, a pair of twins bought kits from the five most popular DTC companies in 2018, and "despite having virtually identical DNA[,]" received no matching results from any of the companies.[257] Similarly, though police arrested DeAngelo on suspicion of being the Golden State Killer, their genetic explorations first led them to believe that a seventy-three-year-old man in

251. *See DNA Database*, N.C. DEP'T OF JUSTICE, https://ncdoj.gov/crime-lab/dna-database/ (last visited May 27, 2020).

252. *See* Molteni, *supra* note 70.

253. *See id.*

254. D.H. Kaye, *Behavioral Genetics Research and Criminal DNA Databases: Laws and Policies*, *in* THE IMPACT OF BEHAVIORAL SCIENCES ON CRIMINAL LAW 355, 356 (Nita Farahany, ed., 2009).

255. *See* Douglas Starr, *Forensics Gone Wrong: When DNA Snares the Innocent*, SCI. (Mar. 7, 2016, 10:00 AM), http://www.sciencemag.org/news/2016/03/forensics-gone-wrong-when-dna-snares-innocent.

256. *See id.*

257. *See* Charlsie Agro and Luke Denne, *Twins Get Some 'Mystifying' Results when They Put 5 DNA Ancestry Kits to the Test*, CBC NEWS (Jan. 18, 2019, 4:00 AM), https://www.cbc.ca/news/technology/dna-ancestry-kits-twins-marketplace-1.4980976.

Oregon instead matched the Killer's DNA.[258] Investigators obtained the Oregon man's DNA from his bed at a rehabilitation center, as he was unable to answer questions due to poor health.[259] Investigators in that instance did obtain a court order for the DNA, but that order was granted based on a match at a "rare genetic marker."[260] But it is unclear whether that marker is, in fact, "rare" or for how long scientists will classify it as such.

Such quicksand consensus around scientific validity becomes all the more unconvincing considering that searches made via third-party doctrine make no distinction in the type of crime being investigated.[261] It is unknown whether third-party doctrine could be used to obtain valuable genetic information for a mere misdemeanor.[262] Compounding these concerns, there are no best practices or certification procedures for genetic genealogists conducting searches, unlike for analysts running typical forensic tests.[263] As researchers at University College London have noted, "There have been cases in the adoption community where people have been reunited with the wrong parents because of misinterpretation of data. . . . If that can happen in an adoption search, it could also happen in a criminal search, with much more adverse consequences."[264]

B. A Tale of Two Tests: How Pre-Carpenter Third-Party Doctrine Fails DTC Genetic Testing Databases

DTC genetic testing customers have a reasonable expectation of privacy in their DNA and the genetic insights that are gleaned from it because DTC companies mislead consumers in two chief ways. First, consumers are led to believe that their data is used for limited purposes and second, that it is easily anonymized.[265] Nevertheless, both the *Katz* test and the trespass test fail to protect DTC genetic testing data.[266] These unsatisfying results illustrate some of the fundamental issues with the third-party doctrine, namely, its nebulous definitions and multiple, sometimes overlapping strands.

Under *Katz* and the third-party doctrine cases that built upon it, the government conducts a search when it intrudes upon an "expectation of privacy . . . that society is prepared to recognize as 'reasonable.'"[267] Setting aside the circularity

258. *See* Balsamo et al. *supra* note 8.

259. *See id.*

260. *See id.*

261. *See supra* Part IV.

262. *See supra* Part IV.

263. *See* Justin Jouvenal, *The Unlikely Crime-Fighter Cracking Decades-Old Murders? A Genealogist*, WASH. POST (July 16, 2018), https://www.washingtonpost.com/ local/public-safety/in-decades-old-crimes-considered-all-but-unsolvable-genetic-genealogy-brings-flurry-of-arrests/2018/07/16/241f0e6a-68f6-11e8-bf8c-f9ed2e672adf_story.html?utm_term=.620480b9ce3b.

264. *Id.*

265. Eric Ravenscraft, *How to Protect Your DNA Data Before and After Taking an At-Home Test*, N.Y. TIMES (June 12, 2019), https://www.nytimes.com/2019/06/12/smarter-living/how-to-protect-your-dna-data.html.

266. *See supra* Section III.A.

267. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J. concurring).

problem for now,[268] several factors contribute to consumers' expectations of privacy in this context.

First, most DTC genetics companies obfuscate what exactly gets stored in their databases and what "product" customers are actually receiving. This makes it unlikely that lay customers know what information it is that they are "voluntarily" disclosing to third parties when they send in their saliva samples. It also suggests one reason that judicial oversight and ability to request clarification via a warrant requirement is important. Generally speaking, there are two distinct points when consumers may get confused regarding what information DTC companies can and will extract from their samples: (1) prior to point of sale, when customers are deciding whether to buy a spit kit; and (2) after consumers send their saliva samples in, when DTC companies store consumers' data.[269]

Beginning with the choice to buy or take a DTC genetic test, consumers are unlikely to understand the nature of the services they're consuming. A significant part of the problem consumers and courts face in decoding how and when third-party doctrine applies to such data concerns slippery statistical language and ambiguously used scientific terms such as "DNA testing" and "ancestry testing."[270] Here, a warrant requirement might encourage law enforcement agencies to specify the type of test results they are requesting and encourage courts and police to pay greater attention to the different types of information that can be at issue. While a complete taxonomy of relevant genetic concepts and their proper terminology is beyond the scope of this Article, a comprehensive survey of all genetic testing forms may one day be useful when considering which types of tests ought to be exempt from third-party doctrine.

Nevertheless, a consumer might think that they are disclosing genetic data that supports *only* an inference of, say, ancestry, without realizing that those same SNPs or regions of DNA can yield a range of less innocuous personal insights. This is important because it is likely that expectations of privacy are directly proportional to how much sensitive knowledge consumers think can be extracted from their samples. At present, DTC companies are not transparent about what happens to the raw DNA data extracted from that saliva, making it unlikely that consumers are providing meaningful voluntary consent for third-party access.[271] For example, 23andMe's Biobanking Consent Document states that it will store "*either* your saliva sample *or* DNA extracted from your saliva," but it is not clear

268. That is, whether or not the courts' rulings cannot be disentangled from those expectations, and whether the question is an empirical one or something more normative.

269. *See, e.g.*, Lesley Fair, *DNA Test Kits: Consider the Privacy Implications*, FED. TRADE COMMISSION: CONSUMER INFO. (Dec. 12, 2017), https://www.consumer.ftc.gov/blog/2017/12/dna-test-kits-consider-privacy-implications (describing measures consumers should take before purchasing a DNA test kit); Kevin Loria, *How to Delete Your Data From 23andMe, Ancestry, and Other Sites*, CONSUMERREPORTS.ORG (Jan. 29, 2019), https://www.consumerreports.org/health-privacy/how-to-delete-genetic-data-from-23andme-ancrestry-other-sites/ (explaining that HIPAA privacy laws do not apply to direct-to-consumer DNA kits, resulting in confusion over how samples are used).

270. *See infra* notes 274–78 and accompanying text.

271. *See* James Hazel & Christopher Slobogin, *Who Knows What, and When?: A Survey of the Privacy Policies Proffered by U.S. Direct-to-Consumer Genetic Testing Companies*, 28 CORNELL J. L. & PUB. POL'Y 35, 50–51 (2018).

whether the DNA is removed after a decade alongside the saliva sample.[272] Moreover, although genetic science may not currently be able to yield inferences regarding something like criminality, because, for example, 23andMe stores for a "minimum of one year and a maximum of ten years,"[273] such inferences may soon become possible as scientists learn more about the genome. Again, a warrant requirement would impose critical limitations on the time and place of a police search, and perhaps guard against the possibility of limitless future usage of individuals' genetic information without probable cause.

What customers actually consent to when they first send in a saliva kit is also foggy because consent policies are worded vaguely and change regularly as companies pivot in response to marketplace and regulatory tides.[274] If anything, customers consent only to their de-identified data's use in further research.[275] Science and the law, however, show that DTC companies cannot deliver on their privacy claims. The false promises that many DTC companies are making may thus lead consumers to reasonably expect greater privacy in their saliva samples than they have. For example, in response to media scrutiny after the Golden State Killer's arrest, DTC genetics companies stressed the privacy protections they provide their customers, both as individual buyers and once aggregated within their databases. Representatives from several major companies publicly sought to reassure consumers that they and they alone are in control of their genetic information. Kate Black, 23andMe's privacy officer and corporate counsel, told NBC News that "We do not sell individual customer information, nor do we include any customer data in our research program without an individual's voluntary and informed consent. 23andMe customers are in control of their data—customers can choose to consent, or not to, at any time."[276] Ancestry.com similarly released a statement stating that it did "not sell your data to third parties or share it with researchers without your consent" and "[customers] may request that we delete your data or account at any time."[277]

The way law enforcement has accessed open-source genetic information may also violate many DTC companies' terms of service. Before uploading DNA to GEDmatch, users must check a box "acknowledging 'that any sample you submit is either your DNA or the DNA of a person for whom you are a legal guardian or have obtained authorization to upload their DNA."[278] Investigators in the Golden State Killer case created a fake profile, and the DNA they uploaded was clearly without the suspect's family members' knowledge or consent. This

272. *See Biobanking Consent Document*, 23ANDME, https://www.23andme.com/about/biobanking/ (last visited May 27, 2020).

273. *Cf. id.*

274. *Id.*

275. *Id.*

276. Daniella Silva, *Senator Calls for More Scrutiny of Home DNA Test Industry*, NBC NEWS (Nov. 26, 2017, 7:15 PM), https://www.nbcnews.com/news/us-news/senator-calls-more-scrutiny-home-dna-test-industry-n824031.

277. *Id.*

278. *See* Lillis et al., *supra* note 6.

leaves open the possibility that DTC DNA data obtained directly from DTC companies rather than through an open-source database like GEDmatch might be similarly misused.

And regardless, though DTC companies claim to protect consumers' genetic privacy through the ability to aggregate and anonymize data, they likely cannot make good on such promises. Because it is the literal stuff we are made of, genetic data such as that collected by DTC companies is capable of identifying individuals even after being "anonymized." Scientists have suggested since at least 2008 that it is possible to "accurately and robustly determine whether [the SNP data of] individuals are in a complex genomic DNA mixture."[279] Thus, even if DTC companies had clear consent and privacy policies and anonymized their data as advertised so as to diminish customers' expectations of privacy to a point where third-party doctrine clearly applied, because DNA *cannot* be wholly separated from the individuals it comes from, such application of the doctrine would be invalid regardless.

If nothing else, customers may have an expectation of privacy that protects their genetic testing data from the broad pre-*Carpenter* reach of third-party doctrine because DTC companies have vehemently said that they do not aid police investigations. In the wake of the Golden State Killer case, companies such as 23andMe, Ancestry.com, MyHeritage, and Helix all denied being connected to the investigation, and went on to launch privacy-promising public relations.[280] One Ancestry.com spokeswoman said, "Ancestry advocates for its members' privacy and will not share any information with law enforcement unless compelled to."[281] She also simultaneously stated that Ancestry had never shared data with law enforcement before.[282] Likewise, Andy Kill, a spokesman for 23andMe, told media that it was the company's policy to "resist law enforcement inquiries" and that "23andMe has never given customer information to law enforcement."[283]

Although a court applying *Katz* to DTC DNA data would likely determine there is a reasonable expectation of privacy in its contents, it is unclear whether a court applying the trespass test revived in *Jones* may reach the same result. Unlike in *Jones*, where the police physically placed a GPS tracker on the defendant's car in order to obtain intangible GPS data, here, there would likely not be a physical trespass that occurs.[284] To be sure, courts have held that directly obtaining biological material from a person is unconstitutional in a number of cases,

279. Nils Homer et al., *Resolving Individuals Contributing Trace Amounts of DNA to Highly Complex Mixtures Using High-Density SNP Genotyping Microarrays*, PLOS GENETICS (Aug. 29, 2008), https://journals.plos.org/plosgenetics/article?id=10.1371/journal.pgen.1000167.
1000167; *see* Nicholas Masca et al., *Participant Identification in Genetic Association Studies: Improved Methods and Practical Implications*, 40 INT'L. J. EPIDEMIOLOGY 1629, 1629 (2011); *see also* Matthias Wjst, *Caught You: Threats to Confidentiality Due to the Public Release of Large-Scale Genetic Data Sets*, BMC MED. ETHICS, Dec. 2010 at 1.

280. *See* Farivar, *supra* note 106.

281. *Id.*

282. *Id.*

283. *Id.*

284. *See* United States v. Jones, 565 U.S. 400, 403 (2012).

including ones involving buccal swabs,[285] police efforts to draw blood,[286] and even breathalyzer tests.[287] And, while the Court in *Maryland v. King* held that DNA swab tests as part of the arrest procedure were constitutional, that DNA was obtained *after* individuals had been arrested, and the DNA was used solely for identification purposes.[288] DTC DNA data, as explained here, does far more than merely identify an individual.[289] Again, a warrant requirement would cabin police use of genetic material to identification purposes and if not, would ideally explain why.

Though *King* did not address events without a physical bodily intrusion or "whether the testing of the 13 identifying loci the police later extracted from King's DNA sample required a separate Fourth Amendment analysis," at least one court has since held that genetic analysis of identifying loci *within* an individual's DNA is not a search.[290] Here, partly because DTC companies do not clarify what information it is that they keep (*e.g.* the saliva sample itself, the raw SNP data, and/or the summarized results only), law enforcement likely does not conduct a search under the trespass test.[291] In the DTC context, customers mix and mail their bodily samples themselves, thus eliminating chances for a tangible connection that might otherwise constitute a physical trespass. Presumably, it is more efficient for law enforcement to collect the raw SNP data or final results reports from DTC companies than to re-test the saliva samples.

C. Carpenter *Perpetuates Doctrinal Confusions*

Applying *Carpenter* to the context of DTC genetic testing, I argue that *Carpenter* does not protect sensitive genetic data from warrantless police searches despite consumers' beliefs such data is private. Accordingly, *Carpenter*'s failure to create a methodical test for lower courts to apply shows that third-party doctrine even after *Carpenter* cannot be consistently applied in an age of ubiquitous, massive data gathering. It also suggests that its difficulties in reconciling third-party cases after *Katz* with modern technologies suggest systemic flaws with the Court's current conception of the doctrine. These insights highlight the importance of a warrant requirement and urge the Court to revisit the third-party doctrine more thoroughly.

Carpenter held that people have a reasonable expectation of privacy in the location metadata generated by cell phones, but the Court's use of three novel factors to reach that conclusion was unjustified at best and deeply confusing at worst. The three factors are: "the deeply revealing nature of [cell phone location metadata];" "its depth, breadth, and comprehensive reach;" and "the inescapable

285. *But see* Maryland v. King, 569 U.S. 435, 440 (2013).
286. *See* Missouri v. McNeely, 569 U.S. 141 (2013).
287. *See* Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 616 (1989).
288. *See* Maryland v. King, 569 U.S. 435, 461 (2013).
289. *See supra* Part I.
290. *See* Raynor v. State, 440 Md. 71, 82 (2014) (emphasizing that the 13 loci the police wanted to test were to be used solely for identification purposes).
291. *See* Saey, *supra* note 54.

and automatic nature of its collection."[292] Because the Court did not explain how it chose or weights the *Carpenter* factors, this Article assumes that the three factors are of equal weight.

Application of *Carpenter*'s three factors to DTC genetic testing demonstrates that the third-party doctrine, even as revised, remains ill equipped to account for modern technology. First turning to the "deeply revealing nature" of the data at issue, it is both obvious that genetic data is deeply personal and important, because it differs from the limited forensic DNA data that police currently use. Many of the most popular DTC genetics companies look at millions of SNPs that offer far more detailed genotyping information than the thirteen loci usually used to identify criminals in law enforcement databases.[293] Unlike the loci, which are restricted to sections of "junk" DNA and restricted to being used for identification purposes, SNPs "have a direct influence on our physical attributes (e.g., hair color, eye color, blood type). . . [and] predispositions to various diseases."[294] 23andMe, for example, alleges its SNP data can ultimately combine to create a far more detailed portrait of an individual than their cell-site location data.[295] A partial list of the things the company states it can illuminate include: disease carrier status, previously unknown biological relatives, paternity, ethnic heritage, propensities toward caffeine consumption and lactose digestion, and muscle type.[296] For police to obtain such a wealth of information without a warrant seems to be exactly the reason the Fourth Amendment was ratified.

The Court's discussion of the first factor also does not address why biological data have historically fallen outside the realm of Fourth Amendment protection. As Justice Kennedy noted in his *Carpenter* dissent, "Financial records are of vast scope [and b]anks and credit card companies keep a comprehensive account of almost every transaction an individual makes on a daily basis."[297] Though genetic data is unique in its ability to quickly reveal so many personal insights from a single source of data, it is not unique in its ability to enable the government to make inferences about many deeply private aspects of an individual's life, such as religious preferences, health status and risks, or personality traits. *Carpenter* thus fails to reliably indicate that genetic information, like cell-site location information, may be different enough from old technologies to exempt it from the third-party doctrine. In light of such confusion from the high Court, a warrant requirement would provide a much-needed measure of constitutional protection to consumers.

Moreover, the second *Carpenter* factor (the data's "depth, breadth, and comprehensive reach") is not clearly distinguishable from the first. It, like the first factor, reveals how the Court skirts around "what makes something a distinct

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

293. Humbert, *supra* note 47, at 101.

294. *See id*.

295. *See generally What You Can Learn*, 23ANDME, *supra* note 28.

296. *See id*.

297. *See Carpenter*, 138 S. Ct. at 2232 (Kennedy, J., dissenting) (discussing the contexts of *Smith* and *Miller*).

category of information,"[298] and cannot resolve the question because the multi-faceted nature and sheer size of many modern third-party datasets makes distinctions using these two factors almost impossible.[299] Mass data collection drives much of modern commerce: the saying "If you're not paying, you're the product," has never been more true.[300] Arguably, much (if not most) data held by today's Internet-based companies can reveal significant amounts of sensitive information. While databases of cell-phone metadata or genetic testing results are obvious candidates for records that may feel private to individuals despite some degree of voluntary sharing, other examples of third-party data gathering that cannot be nearly labeled "public" or "private" include data generated by wearable fitness trackers (*e.g.* FitBit), social media accounts, or even a "smart" fridge that tracks one's food preferences and predicted intake.[301] *Carpenter*'s reliance, then, on an argument based on cell phone technology's novel surveillance capabilities cannot endure in the face of rapid innovation and the Internet of Things.

Finally, the third *Carpenter* factor, the "inescapable and automatic nature of [the information's] collection," weighs against finding that DTC genetic testing data is protected by third-party doctrine because, notwithstanding problems with voluntariness and consent, DTC customers do choose to send in their saliva.[302] Such an individual choice to share data is exactly the same kind of conduct that the Court premised third-party doctrine on in *Miller*.[303] But like *Miller*, *Carpenter*, though it stated a person could "[have] a legitimate privacy interest in records held by a third party,"[304] failed to differentiate between information held by a third party, and information that might depend upon a third party for its value.[305] DTC genetic testing is of the latter type because users cannot sequence their own saliva samples and lack the expertise in genomics to interpret their test results. Further, the choice to pay for DTC testing is unlike the unobtrusive, constant data gathering that occurs on people's cell phones. Sending in samples requires several conscious, physical steps, including generating a substantial 2 mL of saliva, mixing it with buffer for the prescribed amount of time, and mailing it in.[306]

The "inescapable and automatic" factor should, however, go towards Fourth Amendment protection in a situation where law enforcement attempts to use third-party doctrine to obtain DTC genetic testing data from a *fourth* party.[307] When DTC customers give over their genetic data to DTC companies, they likely

298. *Id.* at 2234 (noting the Court's holding is premised on "cell-site records being a 'distinct category of information' from other business records" without comprehensively explaining why).

299. *See* Homer et al., *supra* note 279.

300. Paul Bernal, *Data Gathering, Surveillance and Human Rights: Recasting the Debate*, 1 J. CYBER POL. 243, 260 (2016), https://www.tandfonline.com/doi/full/10.1080/23738871.2016.1228990.

301. Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 88 (2014).

302. *See Carpenter*, 138 S. Ct. at 2223.

303. *See Miller*, 425 U.S. at 443.

304. *See Carpenter*, 138 S. Ct. at 2222.

305. *See generally id.*

306. *See How 23andMe Personal Genetic Service Works*, 23ANDME, *supra* note 58.

307. *See Carpenter*, 138 S. Ct. at 2223.

unknowingly expose their data to a wide array of additional parties, and it is unclear whether those additional parties, in turn, may be legally approached by law enforcement directly under third-party doctrine.[308]

Unlike banks or telephone companies, DTC genetic testing companies are also perhaps unique in the extent to which the companies share the data with fourth parties for a profit, though customers are often unaware of that fact. Though many companies go to great lengths to assure their customers that their data is easily cabined and kept private through advertising, privacy policies, and company press releases, the reality is quite different. 23andMe board member Patrick Chung has said publicly, "The long game here is not to make money selling kits, although the kits are essential to get the base level data. . .Once you have the data, [the company] does actually become the Google of personalized health care."[309] Like Google, DTC companies obtain tremendous value from using and selling that data.

Nearly every DTC company "collaborates" with a number of fourth parties for research and business purposes, though it is not clear how many any given company works with, or to what end.[310] 23andMe, for instance, publicizes a partial list of thirteen collaborators including academic institutions, pharmaceutical giants like Pfizer and Genentech, and non-profits.[311] Ancestry, its leading competitor, has a partial list comprised of only three entities, though its joint endeavor with Google subsidiary Calico Life Sciences recently ended.[312] More troublingly, the "companies all also utilize contractors for services such as business analytics and lab work, though, and the names of those providers or which ones have access to genetic information are not readily available."[313] In all these instances, genetic testing data may be "automatically" forwarded from a DTC company to its fourth-party partners, and then, should law enforcement seek to obtain the information from the latter directly, the third *Carpenter* factor could prove useful in limiting the government's surveillance capabilities, and a warrant requirement would significantly ensure it.

D. Reconfiguring Search Doctrine

Though *Carpenter* is a step in the right direction towards renewed Fourth Amendment protections, third-party doctrine cases have tried and failed to clearly delineate the line between public and private information or to explain how "society" reaches a "reasonable" expectation of privacy. Thus, a property-

308. *See id.* at 2262 (Gorsuch, J., dissenting).

309. Michael Grothaus, *How 23andMe is Monetizing Your DNA*, FAST CO. (Jan. 5, 2015), http://www.fastcompany.com/3040356/what-23andme-is-doing-with-allthat-dna.

310. *See* Kristen V. Brown, *What DNA Testing Companies' Terrifying Privacy Policies Actually Mean*, GIZMODO (Oct. 18, 2017), https://gizmodo.com/what-dna-testing-companies-terrifying-privacy-policies-1819158337.

311. *See Research*, 23ANDME, *supra* note 77.

312. *AncestryDNA Research and Collaboration*, ANCESTRY.COM, (201 https://www.ancestry.com/cs/collaborations (last visited May 27, 2020).

313. Brown, *supra* note 310.

based rule such as that mentioned by Justice Gorsuch in *Carpenter*[314] becomes alluring because by deeming third parties to be, custodians or co-owners rather than absolute information overlords, the Court may be able to draw upon case law pre-dating *Katz* to create a revamped third-party doctrine that resolves many of its doctrinal confusions. Specifically, the Court could return to the property law trespass test—where items implicating a property interest were clearly protected, and if not, were fair game for police—but use modern, "reasonable" expectations of privacy to inform what individuals feel they own and develop a more nuanced taxonomy of types of information.[315]

In sum, as a way forward, we might use the Amendment's interactions with property law to outline four realms of physical things and *Katz* and subsequent cases to explain why consumers should have at least a limited property right in their information that protects them from warrantless searches by law enforcement. This might force courts to reckon with the nuances of the types of information gathered by big data-based enterprises, and in doing so, it would promote clarity that the third-party doctrine has lacked. Here, for example, it would be important that courts recognize that genetic testing data might fall under several different information types, depending on what the DTC company actually collects and what police request access to. There are significant differences between the extracted, unprocessed DNA itself, the raw SNP sequencing data, and the interpreted sequencing results—presumably, only the last two levels of information listed implicate hypersensitive personal attributes. In this way, in the context of DTC genetic material, a more nuanced view of what information contains might encourage courts to consider studies that call into question whether deanonymization of genetic information and tissue samples is even possible [316] and allow the Court to reconcile a new third-party rule with cases that have held that DNA in "garbage cases" is generally fair game for warrantless search and seizure.[317]

Finally, as an alternate path entirely, should the Court wish to treat DNA as truly different from other kinds of data, it might reclassify DNA at a more basic level of Fourth Amendment inquiry. In the context of DTC genetic testing and other types of information directly sourced from the human body, it is possible that instead of falling under the category of "effects" or "home," police access to DTC DNA databases might implicate another category enumerated in the Fourth Amendment entirely: namely, "persons." This approach would give the Court an entirely different line of cases to draw upon and may offer it an opportunity to treat genetic material in particular as a unique category while it hammers out a more robust modern version of third-party doctrine.

314. *See Carpenter*, 138 S. Ct. at 2267–72 (Gorsuch, J., dissenting).

315. *See* United States v. Jones, 565 U.S. 400, 412 (2012).

316. *See* Homer et al., *supra* note 279.

317. Holly K. Fernandez, *Genetic Privacy, Abandonment, and DNA Dragnets: Is Fourth Amendment Jurisprudence Adequate?*, 35 HASTINGS CTR. REP. 21 (2005).

V. CONCLUSION

Without legislative safeguards in place, "personal" genetic testing risks becoming a misnomer at best, and an egregious intrusion into deeply private affairs at worst. Thus, the Fourth Amendment's protections are perhaps the only safeguard this hypersensitive data has against potential police misuse, and allowing the government to trawl DTC genetic testing data without a warrant subverts the spirit of the Fourth Amendment. Moreover, that third-party doctrine cannot consistently protect such data reveals fundamental flaws in that doctrine, as applied in an era of omnipresent information-gathering devices and businesses driven by big data analytics. Courts should recognize that Fourth Amendment jurisprudence likely requires law enforcement to obtain a warrant prior to searches of DTC DNA databases. A Fourth Amendment warrant requirement will ensure that searches are limited to ones that conform to the constitutional right to privacy and help develop clearer guides for courts to use when confronted with government requests to access, use, or store genetic data that it was not authorized to collect itself.