Fordham Law Review

Volume 87 | Issue 6 Article 10

2019

Guilt By Genetic Association: The Fourth Amendment and the Search of Private Genetic Databases by Law Enforcement

Claire Abrahamson
Fordham University School of Law

NOTES

GUILT BY GENETIC ASSOCIATION: THE FOURTH AMENDMENT AND THE SEARCH OF PRIVATE GENETIC DATABASES BY LAW ENFORCEMENT

*Claire Abrahamson**

Over the course of 2018, a number of suspects in unsolved crimes have been identified through the use of GEDMatch, a public online genetic database. Law enforcement's use of GEDMatch to identify suspects in cold cases likely does not constitute a search under the Fourth Amendment because the genetic information hosted on the website is publicly available. Transparency reports from direct-to-consumer (DTC) genetic testing providers like 23andMe and Ancestry suggest that federal and state officials may now be requesting access to private genetic databases as well. Whether law enforcement's use of private DTC genetic databases to search for familial relatives of a suspect's genetic profile constitutes a search within the meaning of the Fourth Amendment is far less clear.

A strict application of the third-party doctrine suggests that individuals have no expectation of privacy in genetic information that they voluntarily disclose to third parties, including DTC providers. This Note, however, contends that the U.S. Supreme Court's recent decision in Carpenter v. United States *overwhelmingly supports the proposition that genetic information disclosed to third-party DTC providers is subject to Fourth Amendment protection. Approximately fifteen million individuals in the United States have already submitted their genetic information to DTC providers. The genetic information held by these providers can reveal a host of highly intimate details about consumers' medical conditions, behavioral traits, genetic health risks, ethnic background, and familial relationships. Allowing law enforcement warrantless access to investigate third-party DTC genetic databases circumvents their consumers' reasonable expectations of privacy by exposing this sensitive genetic information to law enforcement without any meaningful oversight. Furthermore, individuals likely*

* J.D. Candidate, 2020, Fordham University School of Law; B.A., 2014, University of St. Andrews. Thank you to Professor Olivier Sylvain, my editor Jon D'Errico, and the editors and staff of the *Fordham Law Review* for their guidance and assistance. I would also like to thank my family, friends, and Asher for their unwavering encouragement and support.

reasonably expect that they retain ownership over their uniquely personal genetic information despite their disclosure of that information to a third-party provider. This Note therefore asserts that the third-party doctrine does not permit law enforcement to conduct warrantless searches for suspects on private DTC genetics databases under the Fourth Amendment.

INTRODUCTION

In January 2019, Jerry Westrom, a fifty-two-year-old male, visited an ice rink to watch his daughter play in a hockey game.[1] Westrom ordered a hot dog at the concession stand and wiped his mouth with a napkin.[2] Unbeknownst to Westrom, Minneapolis law enforcement officers investigating the violent 1993 murder of a thirty-five-year-old woman named Jeanne Anne "Jeanie" Childs were tracking his every move.[3] A Minneapolis homicide detective investigating the crime had previously run DNA samples obtained from the crime scene through a public genealogy website.[4] Either Westrom or one of his relatives had submitted their genealogical profile to

1. Paul Walsh, *Charge: Hockey Dad's Discarded Napkin at Rink Ties Him to 1993 Killing in Twin Cities 25 Years Later*, MINNEAPOLIS STAR TRIB. (Feb. 15, 2019, 5:00 AM), http://www.startribune.com/man-charged-with-murder-in-stabbing-of-minneapolis-woman-in-93/505838292 [https://perma.cc/EQ4M-S2UN].
2. *Id.*
3. *Id.*
4. *Id.*

this public website, and the police honed in on Westrom as a likely suspect for Childs's murder.[5] As soon as the hockey game was over, the police retrieved Westrom's discarded napkin from a trash can and sent it for forensic testing.[6] The DNA obtained from Westrom's napkin matched the DNA samples collected from the Childs crime scene.[7] After over twenty-five years of unsuccessful investigations, Westrom was arrested and charged with Childs's murder.

Westrom represents one of over fifty suspects in unsolved cold cases who have been similarly identified through the use of public genealogy websites in the past year.[8] This burgeoning police practice gained traction in the spring of 2018, when police arrested the "Golden State Killer," a violent serial killer allegedly responsible for more than fifty rapes and twelve murders across the state of California between 1974 and 1986.[9] Paul Holes, an enterprising DNA expert investigating the crimes, used DNA recovered from a 1980 crime scene of a double homicide suspected to have been committed by the Golden State Killer to develop a "genetic profile" of the suspect.[10] Holes then uploaded this genetic profile to GEDMatch,[11] a public genealogy website with a database of more than 650,000 voluntarily uploaded raw genetic profiles exported from private direct-to-consumer (DTC) genetic testing companies[12] like 23andMe[13] and Ancestry.[14]

GEDMatch analyzed the DNA data points of the suspect's profile and, within twenty-four hours, provided Holes with a list of ten to twenty distant relatives of the suspect.[15] Using this information, Holes worked with Barbara Rae-Venter, a well-known family-tree builder, to develop family trees of thousands of potential suspect relatives.[16] One of those family trees

---

5. *Id.*

6. *Id.*

7. *Id.*

8. *See id.*; *see also* Megan Molteni, *The Future of Crime-Fighting Is Family Tree Forensics*, WIRED (Dec. 26, 2018, 8:00 AM), https://www.wired.com/story/the-future-of-crime-fighting-is-family-tree-forensics [https://perma.cc/TV7L-S3QU].

9. *See* Megan Molteni, *The Creepy Genetics Behind the Golden State Killer Case*, WIRED (Apr. 27, 2018, 2:00 PM), https://www.wired.com/story/detectives-cracked-the-golden-state-killer-case-using-genetics [https://perma.cc/BH7T-F3WX].

10. Justin Jouvenal, *To Find Alleged Golden State Killer, Investigators First Found His Great-Great-Grandparents*, WASH. POST (Apr. 30, 2018), https://www.washingtonpost.com/local/public-safety/to-find-alleged-golden-state-killer-investigators-first-found-his-great-great-great-grandparents/2018/04/30/3c865fe7-dfcc-4a0e-b6b2-0bec548d501f_story.html [https://perma.cc/BYS4-47UM].

11. GEDMATCH, https://www.gedmatch.com [https://perma.cc/A4LT-NPSQ] (last visited Apr. 10, 2019).

12. *See* Molteni, *supra* note 9. This Note refers to these companies as "DTC providers."

13. 23ANDME, https://www.23andme.com [https://perma.cc/3AFH-V4BU] (last visited Apr. 10, 2019).

14. ANCESTRY, https://www.ancestry.com [https://perma.cc/2Y9A-K8KK] (last visited Apr. 10, 2019).

15. *See id.*; *see also* Jouvenal, *supra* note 10.

16. *See* Jouvenal, *supra* note 10; *see also* Heather Murphy, *She Helped Crack the Golden State Killer Case. Here's What She's Going to Do Next*, N.Y. TIMES (Aug. 29, 2018), https://www.nytimes.com/2018/08/29/science/barbara-rae-venter-gsk.html [https://perma.cc/SH4U-DDFJ].

included Joseph James DeAngelo, a retired police officer living in California whose age, sex, and place of residence fit the profile for the Golden State Killer.[17] As with Westrom, the Sacramento police subsequently surveilled DeAngelo and collected his DNA from a discarded item.[18] DeAngelo's DNA matched DNA collected from the Golden State Killer's crime scenes, and he was arrested.[19]

Since the arrest of the Golden State Killer, the use of public genealogy websites to identify suspects has become a preeminent method of solving cold cases.[20] Parabon Nanolabs, a Virginia-based forensic analysis company, recently began offering investigative genealogy services using GEDMatch, citing the increasing demand from law enforcement.[21] The databases of public genealogy websites like GEDMatch are limited to those individuals who voluntarily upload their raw genetic data obtained from DTC providers to find relatives.[22] Law enforcement's use of public genealogy websites for identification of suspects likely is not a search under the Fourth Amendment[23] because these open-source databases of voluntarily disclosed raw genetic data are hosted on public websites and therefore are within the "plain view" of law enforcement.[24]

This Note, however, examines whether law enforcement's use of DTC providers' private databases to search for relatives of a suspect genetic profile would constitute a search under the Fourth Amendment. DTC providers typically require that an individual submits "three milliliters of saliva" to compare his or her genetic profile against others in their databases.[25] As a result, law enforcement officers cannot use the same technique as is used with GEDMatch and likely would have to serve DTC providers with a subpoena or search warrant for their consumers' genetic information.[26]

The databases of DTC providers contain approximately fifteen million genetic profiles as opposed to the one million profiles on GEDMatch.[27] Because any one of these millions of profiles could provide a genetic familial match to a suspect in a cold case, it is highly likely that law enforcement will

17. *See* Molteni, *supra* note 9.

18. *See id.*

19. *See id.*

20. *See* Sarah Zhang, *How a Tiny Website Became the Police's Go-To Genealogy Database*, ATLANTIC (June 1, 2018), https://www.theatlantic.com/science/archive/2018/06/gedmatch-police-genealogy-database/561695 [https://perma.cc/G5W9-XZBG].

21. *See* Molteni, *supra* note 8.

22. *See* Zhang, *supra* note 20.

23. U.S. CONST. amend. IV.

24. *See* Horton v. California, 496 U.S. 128, 133 (1990). Pursuant to *Horton*, where "an article is already in [the] plain view [of law enforcement], neither its observation nor its seizure . . . involve any invasion of privacy." *Id.* Therefore, law enforcement officers likely are entitled to search public websites for genetic information germane to their investigations without a warrant under the Fourth Amendment.

25. *See* Molteni, *supra* note 9.

26. *See id.*

27. *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 [https://perma.cc/AAV2-92W4].

pursue investigation of such databases.[28] Indeed, FamilyTreeDNA, a leading DTC provider, recently disclosed to the public that it has been cooperating with the FBI to test genetic profiles of suspects against its genetic databases since the fall of 2018.[29]

The annual "transparency reports" of the two largest DTC providers, 23andMe and Ancestry, state that law enforcement officials have made requests to these companies to investigate stored data about their users, although both assert that they have not provided any genetic information about users in response.[30] The privacy policies of Ancestry and 23andMe each state that "valid legal process" is required for them to produce information to law enforcement about their users.[31] In addition, 23andMe's privacy policy explicitly states that it uses "all practical legal and administrative resources to resist [law enforcement] requests."[32] However, the extent to which these DTC providers can "resist" such requests under the Fourth Amendment remains unclear.

Under the Fourth Amendment, a search that would violate an individual's "reasonable expectations of privacy" generally requires a warrant.[33] The U.S. Supreme Court, nevertheless, has articulated a standard informally known as the "third-party doctrine," which asserts that a person "has no legitimate expectation of privacy in information . . . voluntarily turn[ed] over to third parties."[34] A strict application of the third-party doctrine might suggest that investigating genetic information held by DTC providers is not

28. *See* Elizabeth R. Pike, *Securing Sequences: Ensuring Adequate Protections for Genetic Samples in the Age of Big Data*, 37 CARDOZO L. REV. 1977, 2010 (2016).

29. *See* Salvador Hernandez, *One of the Biggest At-Home DNA Testing Companies Is Working with the FBI*, BUZZFEED (Jan. 31, 2019, 8:52 PM), https://www.buzzfeednews.com/article/salvadorhernandez/family-tree-dna-fbi-investigative-genealogy-privacy [http://perma.cc/W65Y-XD4Y]; *see also* Press Release, FamilyTreeDNA, Connecting Families and Saving Lives (Feb. 1, 2019), https://blog.familytreedna.com/press-release-connecting-families-and-saving-lives [https://perma.cc/M5RV-8VK2].

30. According to 23andMe's transparency report, as of February 15, 2019, 23andMe has received five "user data requests" from law enforcement. *Transparency Report*, 23ANDME, https://www.23andme.com/transparency-report [https://perma.cc/RYB8-BN57] (last visited Apr. 10, 2019). The report states that 23andMe did not produce "user data" in response to any of these requests. *Id.* Between 2017 and 2018, Ancestry received forty-four information requests from law enforcement. *Ancestry 2017 Transparency Report*, ANCESTRY, https://www.ancestry.com/cs/transparency-2017 [https://perma.cc/GVJ7-33D8] (last visited Apr. 10, 2019); *Ancestry 2018 Transparency Report*, ANCESTRY, https://www.ancestry.com/cs/transparency [https://perma.cc/ESR7-4QMM] (last visited Apr. 10, 2019). Ancestry's transparency reports state that it provided information in response to thirty-eight of those forty-four requests over two years but that none of the information provided included genetic information of its consumers. *Ancestry 2017 Transparency Report*, *supra*; *Ancestry 2018 Transparency Report*, *supra.*

31. *See Ancestry Guide for Law Enforcement*, ANCESTRY, https://www.ancestry.com/cs/legal/lawenforcement [https://perma.cc/YC7W-9GGC] (last visited Apr. 10, 2019); *Transparency Report*, *supra* note 30.

32. *See 23andMe Guide for Law Enforcement*, 23ANDME, https://www.23andme.com/law-enforcement-guide [https://perma.cc/VS8V-TWFU] (last visited Apr. 10, 2019).

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

34. Smith v. Maryland, 442 U.S. 735, 743–44 (1979); *see also* United States v. Miller, 425 U.S. 435, 443 (1976).

a Fourth Amendment search because this information has been willingly shared by consumers with a third party.[35] Accordingly, these consumers arguably have no reasonable expectation of privacy in genetic information disclosed to DTC providers.

However, this Note contends that a strict application of the third-party doctrine to genetic information held by third parties is inappropriate. This stored genetic information can reveal medical traits, behavioral tendencies, ethnic backgrounds, and familial associations of millions of individual consumers.[36] The Court has, in different contexts, held that information of this nature is private and constitutionally protected from government intrusion.[37] Individuals therefore maintain a reasonable expectation of privacy in their genetic information despite disclosing it to a DTC provider for analysis.

Part I evaluates DTC providers' services and privacy policies by using two of the largest DTC providers, 23andMe and Ancestry, as exemplars. Part I also compares the databases of DTC providers against the Combined DNA Index System (CODIS), the national DNA database typically used by law enforcement to identify suspects, to demonstrate that searches of DTC genetic databases circumvent meaningful federal and state law limits placed on law enforcements' searches on CODIS. Part II outlines Fourth Amendment jurisprudence and the applicability of the third-party doctrine. Part III applies the third-party doctrine, and the conflicting approaches to it, to the disclosure of genetic information to third-party DTC providers.

Ultimately, in Part IV, this Note asserts that genetic information disclosed to a DTC provider is not subject to the third-party doctrine. It concludes that a court, if confronted with this issue, should clearly articulate that the practice of investigating genetic information held by DTC providers is presumptively a search under the Fourth Amendment.

I. GENETIC DATABASING BY LAW ENFORCEMENT AND DTC GENETIC PROVIDERS

Members of law enforcement typically search genetic databases only when they cannot obtain matches for a suspect's DNA in CODIS, which is operated by the FBI in cooperation with law enforcement from every state.[38] This Part provides a comparison of the differences between CODIS and DTC genetic databases as a necessary backdrop for understanding the theoretical policy implications of allowing law enforcement unfettered access to investigate private genetic databases.

35. *See infra* Part III.B.1.

36. *See infra* Part I.B.2.

37. *See infra* Part II.B.2.a.

38. *See* Sonia M. Suter, *All in the Family: Privacy and DNA Familial Searching*, 23 HARV. J.L. & TECH. 309, 316 (2010); Natalie Ram, *You Can't Hide Your Genes*, SLATE (May 4, 2018, 11:42 AM), https://slate.com/technology/2018/05/consumer-genetic-databases-arent-the-only-side-door-for-police-to-get-your-dna.html [https://perma.cc/4TWH-ZKJW].

Part I.A examines the legal limitations imposed by federal and state law on the scope of information available in CODIS's DNA databases and law enforcement's use of CODIS. Part II.B describes the services that DTC providers offer. This Part makes clear that, in contrast to CODIS, DTC providers are subject to little regulatory oversight. As such, Part II.B explains that the primary limits on DTC providers' collection and sharing of consumer data inhere in their individual privacy policies and terms and conditions of use.

A. CODIS and "Junk" DNA Searches

Congress authorized the creation of a National DNA Index System (NDIS) in the DNA Identification Act of 1994.[39] Four years later, CODIS, the software program containing this national DNA database, was made available to law enforcement.[40] Local, state, and federal forensic labs upload DNA profiles to CODIS, and the system is monitored by the FBI.[41]

Various state and federal laws limit whose and what type of DNA may be uploaded to CODIS. In addition, law enforcement searches for familial DNA matches on CODIS are subject to legal restrictions.

CODIS is composed of several sub-indices of searchable DNA databases.[42] The indices that are typically used to identify suspects in crimes are the "Forensic Index" and the "Offender Index."[43] The Forensic Index contains genetic profiles of "unknown origin gathered from crime scenes."[44] The Offender Index contains "genetic profiles from the pool of individuals compelled [by law enforcement] to provide genetic samples."[45]

State and federal law specify the circumstances in which law enforcement may compel an individual to subject themselves to a DNA test. All fifty states have laws requiring the collection of DNA from convicted felons, and twenty-eight states authorize the collection of DNA from certain arrestees.[46] Federal law likewise authorizes the collection of DNA from arrestees and convicted felons.[47] As of January 2019, CODIS contained approximately

39. 34 U.S.C. § 12592 (2012).

40. *See* ERIN E. MURPHY, INSIDE THE CELL: THE DARK SIDE OF FORENSIC DATA 14–16 (2015).

41. *See* Erin E. Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291, 295–96 (2010); *see also* Suter, *supra* note 38, at 315–16.

42. *See* Murphy, *supra* note 41, at 296.

43. *See* Suter, *supra* note 38, at 315–16.

44. Murphy, *supra* note 41, at 296.

45. Suter, *supra* note 38, at 316.

46. *See* Julie Samuels et al., *Collecting DNA from Arrestees: Implementation Lessons*, NAT'L INST. JUST. J., June 2012, at 18, 20–21. Notably, of the twenty-eight states authorizing arrestee DNA collection, only thirteen states "collect from all persons arrested for any felony crime, while the other . . . states limit collection to a subset of felonies that typically involve violence or sexual assault." *Id.*; *see also* Maryland v. King, 569 U.S. 435, 451–64 (2013) (holding that a Maryland statute authorizing the collection and storage of arrestees' DNA was constitutional because (1) the collection and storage of arrestees' DNA in CODIS serves legitimate state interests, and (2) arrestees have a diminished expectation of privacy as compared to the public at large).

47. *See* 34 U.S.C. § 40702 (2012).

17.1 million DNA profiles of convicts and arrestees and 915,000 forensic profiles.[48]

Neither the FBI nor any other government agency publishes information regarding the racial distribution of offender profiles in CODIS.[49] However, publicly available reports on the racial composition of arrestees and convicted felons in the United States suggest that approximately 41 to 49 percent of the profiles in the Offender Index likely are of African American individuals.[50] As a result, an estimated "8.6 percent of the entire African American population is currently in the database, compared with only 2 percent of the white population."[51] Similarly, Hispanic males are approximately three times more likely to be incarcerated than white males and therefore have greater representation in CODIS.[52]

Only certain types of DNA are stored in CODIS's databases. Forensic DNA testing uses a method referred to as single-tandem repeat (STR) typing, which analyzes thirteen different "loci" along strands of an individual's genome.[53] Notably, the Court and the medical community at large have referred to these loci as "nonprotein coding junk regions of DNA"[54] because they do not contain genetic material that is "presently recognized as being responsible for trait coding."[55] Therefore, these STR loci theoretically do not reveal any genetic traits associated with race, sex, medical diseases, or other genetic predispositions.[56]

Once a DNA profile of an arrestee or convict is entered into CODIS, law enforcement can compare the offender's DNA profile against suspect DNA profiles, stored in the Forensic Index, that are linked to particular crime scenes.[57] An "Offender Candidate Match," or identification of a suspect linked to a crime scene, is present where the DNA profile from a crime scene matches the offender's DNA profile at all loci.[58]

However, law enforcement officers also perform familial searches in CODIS to identify suspects. The first type of familial search occurs where

48. *CODIS—NDIS Statistics*, FBI.GOV (Jan. 2019), https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics [https://perma.cc/4S54-KNP3].

49. *See* SHELDON KRIMSKY & TANIA SIMONCELLI, GENETIC JUSTICE: DNA DATA BANKS, CRIMINAL INVESTIGATIONS, AND CIVIL LIBERTIES 257 (2010).

50. *Id.* at 258.

51. *Id.*

52. *See* Murphy, *supra* note 41, at 322.

53. *Id.* at 295.

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

55. United States v. Kincade, 379 F.3d 813, 818 (9th Cir. 2004).

56. *See King*, 569 U.S. at 443; *see also* MURPHY, *supra* note 40, at 217. *But see Kincade*, 379 F.3d at 818, 850 (stating that "[b]ecause there are observed group variances in the representation of various alleles at the STR loci . . . DNA profiles derived by STR may yield probabilistic evidence of the contributor's race or sex"). In addition, the court later noted that DNA analysis of STRs could potentially reveal "the presence of traits for thousands of known diseases, and countless numbers of diseases which are currently unknown." *Id.*

57. *See* Murphy, *supra* note 41, at 296.

58. *See* FBI LAB., NATIONAL DNA INDEX SYSTEM (NDIS) OPERATIONAL PROCEDURES MANUAL 54–56 (2018), https://www.fbi.gov/file-repository/ndis-operational-procedures-manual.pdf/view [https://perma.cc/6MU8-D9CQ]; *see also* Suter, *supra* note 38, at 314.

an officer runs an offender profile through CODIS and it is a "partial match" to a suspect DNA profile derived from a crime scene.[59] A partial match suggests that the offender profile may be a "close biological relative" of the suspect DNA profile and narrows the pool of likely suspects.[60] In addition, law enforcement may perform "intentional" familial searches.[61] If the police have an existing suspect who cannot be compelled to provide DNA, they may "attempt to obtain the suspect's DNA indirectly by analyzing DNA from his family members" and comparing those family members' samples to the DNA sample from the crime scene.[62]

B. DTC Genetic Testing Providers' Databases

DTC providers have an expansive database of information related to voluntary consumers of their genetic testing services and typically test for a wider scope of genetic markers than those tested by law enforcement for CODIS. This section focuses on Ancestry and 23andMe, two of the leading DTC providers, to illustrate the scope of private genetic databases and the policies typically surrounding their use.

Part I.B.1 provides statistics on each company's consumer base, and Part I.B.2 clarifies the type of genetic information that these companies test for. Next, Part I.B.3 describes the privacy policies and terms of use that consumers enter into when disclosing their genetic information to DTC providers. Finally, Part I.B.4 describes how the process of conducting familial searches on DTC genetic databases would likely occur.

1. Demographics

Consumer demand for DTC genetic testing has increased exponentially in the past five years. In 2013, 330,000 individuals submitted their DNA for testing to a variety of major DTC providers, including Ancestry and 23andMe.[63] By 2018, the number of individuals who submitted their DNA to DTC providers dramatically increased to approximately 12.275 million.[64] Indeed, in 2017 and 2018 alone, 7.8 million individuals had their DNA tested by DTC providers.[65] Most of the individuals tested are located in the United States, and as a result, an estimated "1 in 25 American adults now have access to [their] personal genetic data."[66]

Recent figures provided by Ancestry and 23andMe suggest that those statistics may already be out of date. Ancestry is the largest DTC provider

59. *See* Suter, *supra* note 38, at 318–19.
60. *Id.* at 319.
61. *See id.* at 326.
62. *Id.* at 320.
63. *See* Antonio Regalado, *2017 Was the Year Consumer DNA Testing Blew Up*, MIT TECH. REV. (Feb. 12, 2018), https://www.technologyreview.com/s/610233/2017-was-the-year-consumer-dna-testing-blew-up [https://perma.cc/A3JS-FV8L].
64. *See id.*
65. *See id.*
66. *See id.*

in the market,[67] and it states that its consumer DNA database is currently composed of over ten million individual profiles.[68] 23andMe follows as the second largest DTC provider, and it has disclosed that approximately five million consumers have submitted their DNA for testing.[69]

DTC providers evidently store the genetic information of a vast number of individuals within their databases. Notably, however, most of these consumers are Americans of European descent.[70] Specifically, nearly 80 percent of individuals in databases from genetic studies tend to be of European descent.[71] By comparison, individuals of East Asian ancestry are the second most prevalent, at only 9 percent, and likely less than 4 percent of individuals in genetic databases are of neither European nor Asian descent.[72]

2. Scope of Information

23andMe and Ancestry both require that individuals seeking testing services provide a sample of their saliva for testing.[73] The companies' laboratories then use that saliva sample to test the "coding" regions of the consumer's DNA for single nucleotide polymorphisms (SNPs).[74] SNPs are "variations in the DNA sequence at particular locations" which "generate biological variation between people."[75] The variations in the genome revealed by SNPs have been statistically correlated with certain "medical conditions, behavioral differences, and even 'recreational' traits (like curly hair or a preference for cilantro)."[76]

Ancestry and 23andMe therefore acquire two forms of data from their consumers: (1) the saliva provided by the consumer (the "biological sample"); and (2) the genetic test results derived from that sample (the

67. *See id.*

68. *Company Facts*, ANCESTRY, http://www.ancestry.com/corporate/about-ancestry/company-facts [https://perma.cc/X8GG-7GYT] (last visited Apr. 10, 2019).

69. *See About Us*, 23ANDME, https://mediacenter.23andme.com/company/about-us [https://perma.cc/DUZ7-Y72X] (last visited Apr. 10, 2019).

70. *See* Brian Resnick, *How Your Third Cousin's Ancestry Test Could Jeopardize Your Privacy*, VOX (Oct. 15, 2018, 10:20 AM), https://www.vox.com/science-and-health/2018/10/12/17957268/science-ancestry-dna-privacy [https://perma.cc/794W-676G]; *see also* 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 [https://perma.cc/S82M-TEAZ].

71. *See* Zhang, *supra* note 70; *see also* Joannella Morales et al., *A Standardized Framework for Representation of Ancestry Data in Genomics Studies, with Application to the NHGRI-EBI GWAS Catalog*, GENOME BIOLOGY, Feb. 15, 2018, at 4, https://genomebiology.biomedcentral.com/track/pdf/10.1186/s13059-018-1396-2 [https://perma.cc/KB4F-R5A3].

72. *See* Morales et al., *supra* note 71, at 4.

73. *See* Molteni, *supra* note 9.

74. *See What Are SNPs?*, 23ANDME, https://www.23andme.com/gen101/snps [https://perma.cc/3SWZ-69DR] (last visited Apr. 10, 2019); *see also AncestryDNA—Frequently Asked Questions (United States)*, ANCESTRY, https://www.ancestry.com/dna/en/legal/us/faq [https://perma.cc/T4B7-AYLF] (last visited Apr. 10, 2019).

75. *See What Are SNPs?*, *supra* note 74.

76. Natalie Ram, *DNA by the Entirety*, 115 COLUM. L. REV. 873, 884 (2015).

"genetic information").[77] The nature of the genetic information available in these databases, however, depends on what type of genetic testing services the company provides.

DTC providers tend to offer two types of personal genetic testing services: ancestral analyses and medical analyses.[78] The ancestral analyses purport to reveal evidence of an individual's ethnic background based on certain genetic markers.[79] In addition, these tests reveal any direct or distant relatives of the individual in their databases who have similarly submitted their genetic material for analysis.[80]

Medical genetic tests performed by DTC providers typically analyze an individual's DNA for a host of genetic variants associated with certain diseases or medical conditions.[81] Ancestry does not offer medical genetic tests to the public at this time.[82] 23andMe, however, offers medical testing services as an add-on to its standard ancestry DNA test for an increased price.[83] 23andMe's medical DNA tests identify whether the individual has any genetic variations that are statistically associated with certain "health risks," like late-onset Alzheimer's disease, celiac disease, Parkinson's disease, and the BRCA1 and BRCA2 gene mutations associated with an increased risk of breast cancer in women.[84] In addition, 23andMe tests the individual's DNA to determine if they are a "carrier" for certain inherited conditions like cystic fibrosis or sickle cell anemia.[85]

Accordingly, DTC providers like Ancestry and 23andMe hold within their databases detailed information regarding millions of their consumers' ethnic, familial, and, in some cases, medical backgrounds.

---

77. *See Privacy Highlights*, 23ANDME, https://www.23andme.com/about/privacy [https://perma.cc/6EVH-ZKLW] (last visited Apr. 10, 2019); *Your Privacy*, ANCESTRY (Apr. 30, 2018), https://www.ancestry.com/cs/legal/privacystatement [https://perma.cc/D3DF-SZPY].

78. *See* Ram, *supra* note 76, at 888–89.

79. *See Our Services: Ancestry*, 23ANDME, https://www.23andme.com/dna-ancestry [https://perma.cc/7H6P-BQGE] (last visited Apr. 10, 2019); *see also AncestryDNA*, ANCESTRY, https://www.ancestry.com/dna [https://perma.cc/8PXN-AGAD] (last visited Apr. 10, 2019).

80. *See Our Services: Ancestry*, *supra* note 79; *see also AncestryDNA*, *supra* note 79.

81. *See* Ram, *supra* note 76, at 889.

82. Ancestry does have a separate service that is currently in beta testing, AncestryHealth, which allows users to build a family tree that includes familial health history and genetic data. Sarah Buhr, *Ancestry.com Welcomes AncestryHealth to the Family*, TECHCRUNCH, https://techcrunch.com/2015/07/16/ancestry-com-welcomes-ancestryhealth-to-the-family [https://perma.cc/X2L8-PZ3R] (last visited Apr. 10, 2019).

83. *See Health + Ancestry Service*, 23ANDME, https://www.23andme.com/dna-health-ancestry [https://perma.cc/PAL6-2HRJ] (last visited Apr. 10, 2019).

84. *See id.*

85. *See id.*

3. Privacy Policies and Terms of Use

Unlike CODIS, DTC providers are not subject to targeted and comprehensive federal and state regulation.[86] There are federal and state laws regulating "aspects of genetic testing and the resulting genetic data," but these laws are of limited applicability to DTC providers.[87] The "Privacy Rule" of the Health Insurance Portability and Accountability Act (HIPAA) of 1996[88] governs private parties' use and disclosure of "individually identifiable health information," such as genetic information, to private parties and law enforcement.[89] However, DTC providers likely do not qualify as a "covered entity" under HIPAA.[90] The Genetic Information Nondiscrimination Act (GINA) of 2008[91] additionally limits the use and disclosure of genetic information by covered entities.[92] GINA, however, only applies to employers and health insurers and therefore, like HIPAA, does not cover the disclosure of genetic information by DTC providers.[93]

As a result, the privacy policies and terms of use of DTC providers predominantly determine the scope of consumers' rights to their disclosed genetic information and how the provider can use and share that data. In particular, Ancestry and 23andMe reserve certain rights with respect to consumers' biological samples and genetic information.

a. Ownership of Genetic Information

Each company's terms explicitly state that its users retain ownership of the genetic information obtained from their biological samples.[94] However, the

86. James W. 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, 39–42 (2018).

87. *Id.* at 39.

88. Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 26, 29, and 42 U.S.C.).

89. 42 U.S.C. §§ 1320d-1 to 1320d-6 (2012).

90. Pursuant to HIPAA, "covered entities" include "health plans, health care clearinghouses, and . . . any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA." OFFICE FOR CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUMAN SERVS., SUMMARY OF THE HIPAA PRIVACY RULE 2 (2013), https://www.hhs.gov/sites/default/files/privacysummary.pdf [https://perma.cc/6DWK-V836]. However, DTC providers "are usually careful to explain that they are not engaged in health care or the manipulation or provision of health data" in order to exempt themselves from HIPAA coverage. Natalie Ram et al., *Genealogy Databases and the Future of Criminal Investigations*, 360 SCIENCE 1078, 1078 (2018); *see also, e.g.*, *23andMe Genetic Health Risk Reports: What You Should Know*, 23ANDME, https://www.23andme.com/test-info [https://perma.cc/9QE6-DLVL] (last visited Apr. 10, 2019) (stating that "Genetic Health Risk reports . . . do not diagnose cancer or any other health conditions or determine medical action").

91. Pub. L. No. 110-233, 122 Stat. 881 (codified as amended in scattered sections of 26, 29, and 42 U.S.C.).

92. *See* 42 U.S.C. § 2000ff (2012).

93. *See* Ram et al., *supra* note 90, at 1078.

94. Ancestry's terms state that "[y]ou always maintain ownership of your data," but Ancestry reserves the right to "collect, host, transfer, process, analyze, communicate and store your Personal Information (including your Genetic Information)." *Ancestry Terms and*

terms also stipulate that consumers' ownership rights in their genetic information remain subject to each company's rights to analyze, store, and, in some instances, share that genetic information pursuant to its terms of service and privacy policy.[95]

Specifically, each company states that a consumer grants the company a "license" to use his or her provided data, including genetic information, as it sees fit. Ancestry's terms explain that its consumers "grant Ancestry a sublicensable, worldwide, royalty-free license to host, store, copy, publish, distribute, provide access to, create derivative works of, and otherwise use . . . User Provided Content."[96] 23andMe goes one step further and states that its users "assign[] a *perpetual*, *irrevocable*, worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display, distribute, reproduce, edit, reformat, and create derivative works from any [submitted] User Content."[97] Thus, although these DTC providers apparently disavow their ownership rights in consumer genetic information, they nonetheless retain a significant proprietary interest in such information.

b. Disclosure of Genetic Information

Each company's terms of service and privacy policy specifies two circumstances in which a consumer's genetic information might be shared with a third party. First, the companies may, with the consumer's informed consent, share the consumer's genetic information with third-party businesses or partners for "research" purposes.[98] These companies' informed-consent forms specify that any identifying information associated with the genetic information is removed before sharing the data with the third-party research partner or company.[99]

Second, the privacy policies make clear that Ancestry and 23andMe may share a consumer's genetic information with public authorities if required to by law.[100] Both companies state that they require "valid legal process" in

Conditions, ANCESTRY (June 5, 2018), https://www.ancestry.com/cs/legal/termsandconditions [https://perma.cc/7WDQ-L7PY]. 23andMe's terms specify that "[a]ny Genetic Information derived from your saliva remains your information, subject to rights [23andMe] retain[s] as set forth in [the Terms of Service]." *Terms of Service*, 23ANDME, https://www.23andme.com/about/tos [https://perma.cc/TD4W-3T7K] (last visited Apr. 10, 2019).

95. *See supra* note 94.

96. *Ancestry Terms and Conditions*, *supra* note 94.

97. *Terms of Service*, *supra* note 94 (emphasis added).

98. *See Privacy Highlights*, *supra* note 77; *Your Privacy*, *supra* note 77; *see also* Valerie Gutmann Koch, *PGTandMe: Social Networking-Based Genetic Testing and the Evolving Research Model*, 22 HEALTH MATRIX 33, 50 (2012).

99. *See AncestryDNA Informed Consent*, ANCESTRY (July 25, 2018), https://www.ancestry.com/cs/dna-redirect/informedconsent-v4-en [https://perma.cc/Y2RX-F2JN]; *Research Consent Document*, 23ANDME, https://www.23andme.com/about/consent [https://perma.cc/P95U-S8PG] (last visited Apr. 10, 2019).

100. *Privacy Highlights*, *supra* note 77; *Your Privacy*, *supra* note 77.

order to produce information to the authorities.[101] 23andMe states that valid "legal or regulatory process" includes "a valid court order, subpoena, or search warrant for genetic or Personal Information."[102] Ancestry similarly defines "legal process" as broadly including, "e.g., subpoenas [and] warrants."[103] The scope of what sort of legal requests might constitute "valid legal process" under these companies' privacy policies and terms of use consequently appears wide and unclear.

At the time of publication, 23andMe continues to assert that it has not shared any of its consumers' genetic information with law enforcement.[104] Ancestry, however, complied with a 2014 warrant for genetic information in its databases obtained by the Idaho Falls Police Department in connection with the 1996 rape and murder of a local resident named Angie Dodge.[105] Ancestry ran a DNA sample of the suspect through one of its genetic databases and initially provided the police with results of its search.[106] These results revealed a partial genetic match in its databases but not the name of the individual connected to the partial genetic match.[107] A subsequent court order, however, compelled Ancestry to provide the name of the match.[108] It is possible that, should law enforcement seek to find familial matches to a potential suspect's profile on a private genetic database, it would issue a similar request to a DTC provider.

4. Familial Searches

The matches to a suspect's profile on a genetic database typically identify distant relatives of the suspect, such as second or third cousins.[109] For this reason, some scientists have referred to the practice of searching genetic databases for relatives of a suspect as conducting "long-range familial searches."[110]

A 2018 study suggests that long-range familial searches are highly effective in narrowing down lists of potential suspects of European descent.[111] In the study, a group of computer scientists and genetic specialists analyzed a "dataset of 1.28 million individuals who were tested

101. *See Ancestry Guide for Law Enforcement*, *supra* note 31; *23andMe Guide for Law Enforcement*, *supra* note 32.

102. *Privacy Highlights*, *supra* note 77.

103. *Your Privacy*, *supra* note 77. Each company also states that it will attempt to notify consumers of any law enforcement requests unless it is prohibited from doing so by court order. *See Ancestry Guide for Law Enforcement*, *supra* note 31; *23andMe Guide for Law Enforcement*, *supra* note 32.

104. *23andMe Guide for Law Enforcement*, *supra* note 32.

105. Paul Elias, *Law Enforcement Investigators Seek Out Private DNA Databases*, SEATTLE TIMES (Mar. 26, 2016, 8:34 AM), https://www.seattletimes.com/business/law-enforcement-investigators-seek-out-private-dna-databases [https://perma.cc/D4WA-NGLT].

106. *Id.*

107. *Id.*

108. *Id.*

109. *See* Resnick, *supra* note 70.

110. Yaniv Erlich et al., *Identity Inference of Genomic Data Using Long-Range Familial Searches*, 362 SCIENCE 690, 690 (2018).

111. *See generally id.*; Resnick, *supra* note 70.

with a DTC provider."[112] This dataset was manipulated so that any "first cousin and closer relationships" were eliminated from the tested pool of individuals.[113] The study projected that "60% of the searches for individuals of European descent will result in a third-cousin or closer match."[114] As for the relative success of long-range familial searches in identifying suspects, the study asserted that creating family trees and using "demographic information, such as geography, age, and sex," to narrow down suspects typically resulted in a list of sixteen to seventeen potential suspects.[115]

Law enforcement officials ordinarily turn to genetic databases only when they are unable identify a suspect using CODIS or other traditional investigative means.[116] DTC providers are therefore a valuable resource for law enforcement investigations because of their capacity to generate a small suspect pool when no leads have otherwise materialized for months, years, or even decades.

II. THE FOURTH AMENDMENT AND INFORMATION STORED BY THIRD PARTIES

Long-range familial searches on DTC genetic databases are a powerful tool for law enforcement to identify suspects in unsolved crimes. 23andMe and Ancestry, for their part, have either explicitly or implicitly indicated their intent to resist law enforcement requests to investigate their genetic databases.[117] However, whether these companies can demand that law enforcement obtain a warrant to access their stored genetic information depends on whether consumers' privacy interests in their genetic information are protected under the Fourth Amendment.

The Fourth Amendment establishes the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" by the government.[118] This Part outlines the varying understandings of the third-party doctrine that shape the determination of whether law enforcement's use of DTC genetic databases to perform long-range familial searches for suspects would constitute a search under the Fourth Amendment.

Part II.A provides a brief overview of the warrant clause and constitutionally protected realms of privacy under the Fourth Amendment. Part II.B explains how the third-party doctrine affects those privacy interests.

---

112. Erlich et al., *supra* note 110, at 690.
113. *Id.*
114. *Id.* at 690–91.
115. *Id.* at 691.
116. *See* Ram, *supra* note 38.
117. 23andMe states that it "chooses to use all practical legal and administrative resources to resist requests from law enforcement." *23andMe Guide for Law Enforcement*, *supra* note 32. At the time of publication, Ancestry has not issued a similar statement. However, when law enforcement obtained a warrant to search Ancestry for genetic information in 2014, Ancestry asserted that it would only provide deidentified genetic data in the absence of a more explicit warrant. *See* Elias, *supra* note 105.
118. U.S. CONST. amend. IV.

This Part then describes how *Carpenter v. United States*[119] has limited the third-party doctrine by recognizing that it does not apply to privacy interests in certain kinds of information. Finally, this Part details what additional factors courts currently take into consideration in determining whether the third-party doctrine applies to particular forms of data stored by third parties.

A. The Fourth Amendment, Warrants, and Reasonable Expectations of Privacy

The Framers drafted the Fourth Amendment largely in response to Britain's use of general warrants and writs of assistance during the colonial period.[120] General warrants and writs of assistance effectively authorized British officials to conduct "sweeping searches and seizures [of private property at will and] without any evidentiary basis."[121] Accordingly, the Framers intended that the Fourth Amendment protect an individual's privacy interests in his or her property by requiring that the government obtain a warrant supported by "probable cause" before conducting a search or seizure.[122]

Each and every police investigation of an individual and their property is not presumptively a search under the Fourth Amendment.[123] Traditionally, a Fourth Amendment search occurred only where law enforcement physically trespassed upon an individual's private property.[124] However, in *Katz v. United States*,[125] the Court held that the Fourth Amendment protects "people, not places," and, therefore, could not exclusively "turn upon the presence or absence of a physical intrusion into any given enclosure."[126] Instead, the Court held that what an individual "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[127]

Justice John Marshall Harlan, in his concurring opinion in *Katz*, asserted that the majority had set up a two-pronged evaluation for the Fourth Amendment. Harlan specified that the *Katz* analysis requires: (1) "that a person have exhibited an actual (subjective) expectation of privacy"; and (2) "that the expectation be one that society is prepared to recognize as

119. 138 S. Ct. 2206 (2018).

120. *See* Henry v. United States, 361 U.S. 98, 100 (1959); *see also* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 1.1(a) (5th ed. 2017).

121. Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 19, 82 (1988).

122. *See* 2 LAFAVE, *supra* note 120, § 3.1.

123. *See* 1 *id.* § 2.1.

124. *See* 1 *id.* § 2.1(e); *see also, e.g.*, Olmstead v. United States, 277 U.S. 438, 465 (1928) (holding that a wiretap did not constitute a Fourth Amendment search because the tapped "wires [we]re not part of [the defendant's] house or office any more than are the highways along which they are stretched").

125. 389 U.S. 347 (1967).

126. *Id.* at 351, 353.

127. *Id.* at 351.

'reasonable.'"[128] Subsequent Supreme Court jurisprudence has articulated various doctrinal approaches to the "reasonableness" prong under Harlan's test with regard to particular forms of what an individual subjectively deems "private" under the Fourth Amendment.

B. The Applicability of the Third-Party Doctrine in the Information Age

In *Smith v. Maryland*,[129] the Court articulated the standard now known as the third-party doctrine, which holds that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[130] Therefore, an individual gives up "all of his Fourth Amendment rights" in any information disclosed to a third party.[131] Indeed, courts have held that this standard holds true "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[132] Accordingly, under the third-party doctrine, bank records,[133] telephone records,[134] and IP addresses[135] are not protected under the Fourth Amendment and may be obtained by law enforcement from a third party without a warrant.

In *Carpenter*, however, the Court drastically revised its prior stance of strictly precluding information disclosed to third parties from Fourth Amendment protections.[136] While disclosure of information to a third party suggests that an individual has a "reduced expectation of privacy," the Court asserted that possessing "diminished privacy interests" in information does not act as a per se bar to the application of the Fourth Amendment.[137] Individuals do not, the Court specified, abandon all expectations of privacy "by venturing into the public sphere" and engaging with third-party providers.[138] Instead, the Court implied that if disclosures made to a third party have the potential to reveal fundamentally personal and intimate information, an individual has not conclusively forfeited his or her Fourth Amendment privacy interests in the information through the disclosure.[139]

---

128. *Id.* at 361 (Harlan, J., concurring). Harlan further stated that under this conception, any "objects, activities, or statements that [an individual] exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited." *Id*.

129. 442 U.S. 735 (1979).

130. *Id.* at 743–44; *see also* United States v. Miller, 425 U.S. 435, 443 (1976) (holding "that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party").

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

132. *Miller*, 425 U.S. at 443.

133. *See id.* at 442–43.

134. *See Smith*, 442 U.S. at 742–44.

135. *See* United States v. Caira, 833 F.3d 803, 809 (7th Cir. 2016); *see also* United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008).

136. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

137. *Id*. at 2219 (quoting Riley v. California, 134 S. Ct. 2473, 2488 (2014)).

138. *Id.* at 2217.

139. *See id.*

A strict rendering of the third-party doctrine is premised on a theory of assumption of risk by the disclosing party. This assumption-of-risk theory has been supplemented by *Carpenter*'s emphasis on evaluating the nature and scope of particular information provided to third parties. However, there is a minority approach described in *Carpenter* that suggests that expectations regarding proprietary rights in particular forms of information shape an individual's reasonable expectations of privacy in information disclosed to a third party. This alternative approach has strong support in the traditional, property-based conception of the Fourth Amendment.

1. Assumption of Risk and the Strict Application of the Third-Party Doctrine

Assumption of risk is the traditional rationale for strictly excluding information disclosed to third parties from Fourth Amendment protections. As the Court articulated in *United States v. Miller*,[140] an individual "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the government."[141] The underpinnings of this theory are thus relatively simple: when individuals expose their information to a third party, they risk subsequent exposure of that information to a wider net of individuals and entities. Fortunately or not, that wider net may include law enforcement. Because third parties have no "meaningful interests in records sought by a subpoena . . . [they therefore] have no rights to object to the records' disclosure—much less to assert that the Government must obtain a warrant to compel disclosure of the records."[142] As a result, under this approach, law enforcement officials are entitled to investigate any information disclosed to a third-party business without a warrant, regardless of whether the disclosing individual or third party objects.

2. *Carpenter*'s Expansion of Privacy Protections Under the Third-Party Doctrine

In *Carpenter*, the Court rejected the strict application of the third-party doctrine to cell-site records maintained by telephone companies.[143] The Court asserted that, because a cell phone "logs a cell-site record . . . without any affirmative act on the part of the user" and using a cell phone is essential to daily life, it is inappropriate to assume that the user voluntarily assumes the risk of disclosure of his or her cell-site records to law enforcement.[144] Furthermore, Chief Justice Roberts, writing for the majority, contended that

140. 425 U.S. 435 (1976).

141. *Id.* at 443; *see also* Smith v. Maryland, 442 U.S. 735, 744 (1979) (holding that the defendant, in "voluntarily convey[ing] numerical information to [a] telephone company and 'expos[ing]' that information to its equipment in the ordinary course of business . . . assumed the risk that the company would reveal to police the numbers he dialed").

142. *Carpenter*, 138 S. Ct. at 2228 (Kennedy, J., dissenting).

143. *See id.* at 2217.

144. *Id.* at 2220.

the third-party doctrine is not exclusively premised on assumption of risk.[145] Rather, Roberts asserted, the Court additionally had "considered 'the nature of the particular documents sought' to determine whether 'there is a legitimate "expectation of privacy" concerning their contents.'"[146]

The Court then specified that the "depth" and "comprehensive reach" of cell-site data were highly relevant considerations in evaluating the nature of this particular form of information.[147] Paul Ohm, a recognized scholar in information privacy law, has more broadly framed these lines of inquiry in *Carpenter*.[148] Professor Ohm asserts that the "depth" prong in *Carpenter* considers the "detail and precision of the information stored."[149] The "comprehensive reach" prong then specifically addresses the "number of people tracked in the database."[150]

Pursuant to *Carpenter*, if the depth and comprehensive reach of the particular information disclosed to a third party threatens a "too permeating police surveillance" and compromises individuals' personal security, there may be justifiable grounds to designate that information as protected under the Fourth Amendment.[151] The Court also stated that the "deeply revealing nature" of cell-site data, its "breadth," and the "inescapable and automatic nature of its collection" justified protection of such data under the Fourth Amendment.[152]

This Note limits its scope to the "depth" and "comprehensive reach" prongs of the *Carpenter* analysis because the "deeply revealing nature" of the particular form of information is also analyzed as part of the "depth" prong.[153] The considerations of "breadth" and the "inescapable and automatic nature of collection" are addressed to the passive collection by third parties of numerous data points over a prolonged period of time.[154] Because genetic data is collected by DTC providers only once, as a result of an active disclosure by the consumer, these considerations are not applicable to private genetic databases. Parts II.B.2.a and II.B.2.b therefore evaluate only the relevant legal and policy inquiries under the depth and comprehensive reach prongs in greater detail.

---

145. *Id.* at 2219–20.

146. *Id.* at 2219 (quoting *Miller*, 425 U.S. at 442). In *Smith* and *Miller*, the Court ultimately concluded that, because records of checks and telephone logs do not reveal information we distinctly view as private, Fourth Amendment protection of the respective disclosures was unwarranted. *See Smith*, 442 U.S. at 742; *Miller*, 425 U.S. at 442–43.

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

148. Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. (forthcoming 2019) (manuscript at 15), https://osf.io/preprints/lawarxiv/bsedj/ [https://perma.cc/2APS-LT7M].

149. *Id.*

150. *Id.*

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

152. *Id.* at 2223.

153. *See infra* Part II.B.2.a; *see also* Ohm, *supra* note 148 (manuscript at 15).

154. *See* Ohm, *supra* note 148 (manuscript at 15, 19–21).

a. Depth of Information Available in Third-Party Databases

The *Carpenter* Court ultimately declined to extend the third-party doctrine to cell-site records held by phone companies because these records, by revealing every single locale an individual visits each day, inappropriately provided the government with "an intimate window into a person's life."[155] In making this determination, the Court relied on Justice Sotomayor's observation, in her concurring opinion to *United States v. Jones*,[156] that "a precise, comprehensive record of a person's public movements [reveals] a wealth of detail about her familial, political, professional, religious, and sexual associations" and that there are associated risks of granting the government access to such intimate records.[157]

Justice Sotomayor implied in *Jones* that a Fourth Amendment analysis should consider whether the data held by a third party reveals information that is more broadly recognized by the Court as "private" under the U.S. Constitution and consequently outside the scope of information that the government should have unfettered access to.[158] For example, the Court has consistently deemed that intimate details regarding familial decision-making and sexual behavior are within a "zone of privacy" protected by the Bill of Rights, which must remain free from "governmental intrusion."[159] Comprehensive records of an individual's physical movement, in theoretically revealing to the government that she visited "[an] abortion clinic, [an] AIDS treatment center . . . [or] a gay bar," therefore potentially implicated those constitutionally recognized realms of sexual and familial privacy.[160] Sotomayor thus suggested in *Jones* that if the "depth" of information revealed by location-based records is inherently private under the Constitution, law enforcement could not obtain such information without a warrant under the Fourth Amendment.

b. Comprehensive Reach of Third-Party Databases

In *Carpenter*, the Court suggested that the third-party doctrine should not be applied to information databases with a reach that could permit the government to surveil substantially all, or a vast majority of, people in the

155. *Carpenter*, 138 S. Ct. at 2217.
156. 565 U.S. 400 (2012).
157. *Id.* at 415 (Sotomayor, J., concurring).
158. *See id.*
159. *See* Griswold v. Connecticut, 381 U.S. 479, 483–85 (1965) (holding that the "sacred precincts of [the] marital bedroom" are not subject to government intrusion); *see also, e.g.*, Obergefell v. Hodges, 135 S. Ct. 2584, 2599 (2015) (protecting "personal choice regarding marriage" from government intrusion); Lawrence v. Texas, 539 U.S. 558, 567 (2003) (protecting sexual behavior from government intrusion); Eisenstadt v. Baird, 405 U.S. 438, 453 (1972) (protecting the decision to procreate from government intrusion); Prince v. Massachusetts, 321 U.S. 158, 166 (1944) (protecting the "private realm of family life" from government intrusion).
160. *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) (quoting People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009)).

United States.[161] Roberts's assertion is strongly supported by an originalist perspective on the Fourth Amendment. As stated previously, a primary object of the Framers in drafting the Fourth Amendment was to foreclose widespread searches of individuals and their property by the government without probable cause.[162] In another case, Justice Antonin Scalia asserted that the Framers therefore intended for the Fourth Amendment to prohibit suspicionless searches of individuals if their "principal end is ordinary crime-solving."[163] Instead, Scalia contended that, absent "special needs," individualized suspicion of criminal guilt was necessary to conduct a search.[164]

The third-party doctrine risks allowing government officials to conduct suspicionless searches with impunity by permitting the collection and indefinite retention of intimate, third-party data on millions of private citizens. As Daniel Solove, a scholar in privacy and information security, has stated, "as more private sector data becomes available to the government, there could be a de facto national database, or a large database of 'suspicious' individuals," that law enforcement officials could search at will.[165] The judiciary, therefore, may additionally consider the privacy risks of allowing the government unrestricted access to search the personal information of an extremely wide breadth of individuals, without individualized suspicion, in evaluating whether the third-party doctrine applies.

3. Proprietary Interests in Information Stored by Third Parties

An alternative to the majority approach in *Carpenter* calls for premising the applicability of the third-party doctrine on the proprietary interests of the disclosing individual in his or her information. Justice Anthony M. Kennedy, in his *Carpenter* dissent, criticized the majority's assertion that *Miller* and *Smith v. Maryland*[166] permitted a content-based analysis of the disclosed information to determine if the third-party doctrine applies.[167] Instead, Kennedy contended, at the crux of the third-party doctrine is the notion that that individuals must have a "sufficient connection to the thing or place searched to assert Fourth Amendment interests in it."[168] He asserted that property concepts bear heavily on the determination of whether individuals maintain this requisite "connection" to information held by a third party.[169]

161. *See* United States v. Carpenter, 138 S. Ct. 2206, 2218 (2018).
162. *See supra* Part II.A.
163. Maryland v. King, 569 U.S. 435, 469 (2013) (Scalia, J., dissenting).
164. *Id.* at 469–70.
165. Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1107 (2002).
166. 442 U.S. 735 (1979).
167. United States v. Carpenter, 138 S. Ct. 2206, 2224 (2018) (Kennedy, J., dissenting). Justice Kennedy asserted that, to the contrary, the Court in both cases affirmed that the third-party doctrine applies "even when the records contain personal and sensitive information." *Id.* at 2223.
168. *Id.* at 2227.
169. *Id.*

Kennedy's return to a property-based conception of reasonable expectations of privacy was not without modern precedent. In *United States v. Jones*, Justice Scalia criticized interpretations of *Katz* that suggest its analysis foreclosed a consideration of an individual's property interests under the Fourth Amendment.[170] By contrast, Scalia asserted, *Katz*'s call for judicial evaluation of the "reasonableness" of an individual's subjective expectations permits a consideration of "*either* . . . concepts of real or personal property law *or* . . . understandings that are recognized and permitted by society."[171] Concepts of property law therefore may inform whether an individual maintains a reasonable expectation of privacy in information disclosed to and held by a third party.[172] Where, as part of the transaction with the third party, an individual does not "own, possess, control, or use the records" held by the third party, Kennedy asserted, he or she has "no reasonable expectation that [those records] cannot be disclosed pursuant to lawful compulsory process."[173]

Three different concepts of property law predominate in evaluating an individual's reasonable expectations of privacy in particular property. First, the Court has emphasized that an individual maintains an unwavering reasonable expectation of privacy in the sanctity of the home.[174] Specifically, in the home "*all* details are intimate details."[175] Thus, even where the government does not physically intrude in a home but employs "sense-enhancing technology" to obtain intimate details from within the home, an individual's reasonable expectations of privacy have been invaded under the Fourth Amendment.[176]

Second, where an individual grants their property to a third party, the judiciary might consider whether the transaction was merely a bailment to the third party or effected a full transfer of ownership rights.[177] This perspective considers the scope of ownership and use granted to the third party by the individual via the transaction. Kennedy, in his *Carpenter* dissent, asserted that granting a third-party company the right to use and control business records, such as cell-site or other telephone records, was not a bailment and established full abdication of ownership rights to the third party.[178] By contrast, Justice Gorsuch suggested that the entrustment of records to a third party is better understood as a bailment.[179] As a "bailor," an individual does not "lose any Fourth Amendment interest in [his or her data]" by entrusting it to a third party.[180] Indeed, as "bailee," the third party

170. United States v. Jones, 565 U.S. 400, 406–07 (2012).
171. *Id.* at 408 (emphasis added) (quoting Minnesota v. Carter, 525 U.S. 83, 88 (1998)).
172. *See Carpenter*, 138 U.S. at 2227 (Kennedy, J., dissenting).
173. *Id.* at. 2224.
174. *See* Payton v. New York, 445 U.S. 573, 585 (1980); *see also* Kyllo v. United States, 533 U.S. 27, 34–38 (2001).
175. *Kyllo*, 533 U.S. at 37.
176. *Id.* at 34.
177. *See Carpenter*, 138 S. Ct. at 2228 (Kennedy, J., dissenting).
178. *Id.*
179. *See id.* at 2268–69 (Gorsuch, J., dissenting).
180. *Id.* at 2269.

should protect the bailor's private property to the extent the bailor likely would deem necessary.[181] Third parties, as bailees, consequently might have the standing to require that law enforcement obtain a warrant to search property within their databases pursuant to the Fourth Amendment.

Finally, existing sources of positive law that specify ownership rights in certain forms of information necessarily shape the disclosing party's reasonable expectations of privacy.[182] As Gorsuch asserts, if federal or state law specifies that customers retain a proprietary interest in certain forms of information that might be disclosed to third parties, such laws should govern an individual's reasonable expectations of privacy in that information.[183]

III. APPLICATION OF THE THIRD-PARTY DOCTRINE TO GENETIC INFORMATION DISCLOSED TO DTC PROVIDERS

At the time of publication, a law enforcement request to access genetic information from a DTC provider has not been challenged in court. However, if law enforcement officials attempt to acquire such data in the future, larger DTC providers like 23andMe and Ancestry will presumably use their collective legal might to resist such requests and protect consumer trust in their multimillion-dollar genetic testing enterprises.[184] In addition, it is possible that an individual implicated by a relative's genetic information in a DTC genetic database might attempt to exclude that evidence from trial. It is therefore reasonably probable that the judiciary will have to determine whether genetic information voluntarily disclosed to a DTC provider is subject to Fourth Amendment protections in the near future. This Part applies the conflicting theories surrounding the third-party doctrine articulated in Part II.B to the disclosure of genetic information to a third-party DTC provider.

Part III.A specifies the individuals and entities whose privacy interests are likely implicated through investigations of DTC genetic databases. Part III.B analyzes how a strict application of the third-party doctrine could suggest that law enforcement's investigation of genetic information held by DTC providers does not constitute a search under the Fourth Amendment. Finally, Part III.C examines the alternative perspective that the third-party doctrine does not apply to stored genetic data given the sensitive nature of information revealed by genetic material and the relative proprietary interests associated with disclosed genetic information.

181. *Id*.
182. *Id.* at 2270.
183. *Id.*
184. As Orin Kerr has asserted, consumer trust is key to the business model of many third-party providers and such providers are therefore often willing to go to court to protect consumer data. *See* Kerr, *supra* note 131, at 598.

A. Privacy Interests at Stake in Law Enforcement Investigations of DTC Genetic Databases

As a threshold matter, it is important to note whose privacy interests are potentially implicated by law enforcement searches of DTC providers. Sonia Suter, a scholar in bioethics and genetic privacy, has identified three different entities whose privacy interests are implicated in the related context of familial searches in CODIS[185]: (1) the "genetic informant" or "pivot person" whose DNA is in CODIS and provides a partial match to a DNA sample from a crime scene (the "Informant");[186] (2) the relatives of the Informant who are investigated as suspects as a result of the partial match in CODIS (the "Targets");[187] and (3) the "family unit as a whole," whose intimate familial ties are subject to investigation by law enforcement (the "Collective").[188]

While Professor Suter was writing about CODIS, her categorization can be applied to law enforcement searches of DTC genetic databases. Here, the Informant is the individual who provides his or her genetic information to a third-party DTC provider. The Target is the "fourth-party" relative who is unwittingly implicated as a result of his or her family member submitting her genetic information to a DTC provider. Finally, the Collective is the entire familial unit who shares varying degrees of genetic material with the Informant and the Target. This Note focuses on the Informant's privacy interests because his or her disclosure to the DTC provider potentially triggers the third-party doctrine.[189] However, the privacy interests of the Target and the Collective may impact the analysis in terms of reasonable expectations of privacy regarding familial relationships and genetic information. In addition, the interests of the Collective may bear on relative proprietary interests in the disclosed genetic information.

B. The Third-Party Doctrine as Applicable to Genetic Information: Law Enforcement's Right to Perform Warrantless Searches

Law enforcement officials seeking to perform warrantless searches of DTC providers' databases would likely argue that the Informant cannot claim

185. Suter, *supra* note 38, at 328.
186. *Id.*
187. *Id.*
188. *Id.*
189. Notably, there are standing problems that would prevent these three entities from bringing a Fourth Amendment claim. The Informant likely would not have standing to invoke the exclusionary rule in court. *See* Rakas v. Illinois, 439 U.S. 128, 134 (1978) (holding that "it is proper to permit only [criminal] defendants whose Fourth Amendment rights have been violated to benefit from the [exclusionary] rule's protections"). Similarly, the Target can only allege that evidence should be excluded as an illegal search under the Fourth Amendment if *his or her* Fourth Amendment rights have been violated. *See id.*; *see also* Murphy, *supra* note 41, at 33. The standing issue is outside the scope of inquiry of this Note; however, both Erin Murphy and Mary Coombs have made powerful arguments that the Target should have standing to assert his or her Fourth Amendment right to protect shared privacy interests with the Informant, or on behalf of the privacy interests of the Informant. *See* Murphy, *supra* note 41, at 336. *See generally* Mary I. Coombs, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 CALIF. L. REV. 1593 (1987).

any reasonable expectation of privacy in genetic information voluntarily disclosed to a DTC provider. As a result, law enforcement would not be required to obtain a warrant supported by probable cause to request genetic information from DTC providers.

The assumption-of-risk theory underlying the third-party doctrine supports the notion that the Informant maintains no reasonable expectation of privacy in disclosed genetic information. Furthermore, the alternative approaches to the applicability of the third-party doctrine that are articulated in *Carpenter* do not alter the analysis in the context of genetic databases.

1. Assumption of the Risk of Law Enforcement Exposure

A strict application of the third-party doctrine pursuant to *Smith* and *Miller* could suggest that the Informant voluntarily assumes the risk of disclosure of his or her genetic information to law enforcement through interacting with a DTC provider. Indeed, consumers who provide their genetic information to third-party providers potentially waive, both implicitly and explicitly, any reasonable expectation of privacy in that data.

On the one hand, implicit in the Informant's act of submitting a biological sample to a DTC provider is the subsequent exposure of his or her genetic information to a wide range of entities.[190] This scope of exposure includes the DTC provider, external labs that analyze the Informant's biological sample, and any consumer who shares genetic information with the Informant and similarly has submitted their genetic information for testing to the company.[191] Furthermore, the Informant often consents to an even wider net of exposure when he or she provides informed consent to share the disclosed genetic information with external research and business partners.[192] Although this information is technically deidentified when shared with the third party, extensive media coverage suggests that it is relatively easy for such genetic information to be "deanonymized" by scientists.[193] Pursuant to *Smith* and *Miller*, then, the Informant has voluntarily assumed the risk that any number of those individuals or entities could reveal his or her genetic information to the authorities.[194]

On the other hand, volitional assumption of risk need not be implied because the Informant explicitly contracts with the DTC provider to accept

190. *See supra* Part I.B.3.

191. *See supra* Part I.B.3.

192. *See supra* Part I.B.3.

193. *See, e.g.*, Peter Pitts, *The Privacy Delusions of Genetic Testing*, FORBES (Feb. 15, 2017, 1:26 PM), https://www.forbes.com/sites/realspin/2017/02/15/the-privacy-delusions-of-genetic-testing [https://perma.cc/84VP-WB2N]; *see also* Ifeoma Ajunwa, Opinion, *Can a Genetic Test Be Anonymous?: There's No Guarantee of Anonymity*, N.Y. TIMES: ROOM FOR DEBATE (Mar. 4, 2017, 7:22 PM), https://www.nytimes.com/roomfordebate/2015/03/02/23andme-and-the-promise-of-anonymous-genetic-testing-10/theres-no-guarantee-of-anonymity [https://perma.cc/SA6E-ZE8Q].

194. *See supra* Part II.B.1; *see also* United States v. White, 401 U.S. 745, 751–52 (1971) (holding that information disclosed to a third-party individual who later becomes a police informant is not protected under the Fourth Amendment).

the risk of exposure of his or her genetic information to law enforcement. Prior to ordering a genetic testing kit from 23andMe or Ancestry, the consumer must create an account on the company's website.[195] In creating an account, the consumer is directed to read and consent to the company's terms of use and privacy policies.[196]

On 23andMe, the individual must click a box indicating that they have "read and agree to" the terms of service and privacy policy before creating an account.[197] On Ancestry, a statement indicates that by clicking a box marked "save and continue" the individual agrees to the terms of use and privacy statements.[198] The terms and privacy policies explicitly state that the companies may be required to hand over any information disclosed by the Informant to law enforcement.[199] These "clickwrap" contractual terms are typically binding on consumers, so long as they have adequate notice of terms before they indicate their consent.[200] This informed consent to the risk of law enforcement exposure vis-à-vis the clickwrap terms of DTC providers' consumer contracts therefore arguably establishes voluntary assumption of the risk pursuant to the third-party doctrine.[201]

In addition, the Court in *Carpenter* in part determined that cell-site records were excludable from the third-party doctrine because assumption of risk could not be presumed in the particular context of cell phone usage. Because using a cell phone is "indispensable to participation in modern society,"[202] the Court held that a consumer virtually has no choice but to disclose a variety of highly detailed information to the cell phone provider and therefore does not *voluntarily* assume the risk of exposure of that information to law enforcement.[203]

By contrast, transacting in genetic information with companies like 23andMe and Ancestry is likely not a social or economic necessity. Knowing one's genetic background may impact one's understanding of her ethnic makeup and medical propensities; however, this knowledge is probably not a practical necessity in order to understand one's personhood or function in

195. *See* ANCESTRY, *supra* note 14; 23ANDME, *supra* note 13.
196. *See* ANCESTRY, *supra* note 14; 23ANDME, *supra* note 13.
197. *See* 23ANDME, *supra* note 13.
198. *See* ANCESTRY, *supra* note 14.
199. *See supra* Part I.B.3.
200. Caspi v. Microsoft Network, L.L.C., 732 A.2d 528, 531–32 (N.J. Super. Ct. App. Div. 1999).
201. *See supra* Part II.B.1; *see also* Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973) (holding that it is "well settled that one of the specifically established exceptions to the requirements of both a warrant and probable cause [under the Fourth Amendment] is a search that is conducted pursuant to consent").
202. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018); *see also* Riley v. California, 134 S. Ct. 2473, 2484 (2014); United States v. Miller, 425 U.S. 435, 451 (1976) (Brennan, J., dissenting) (holding that the disclosure of financial records to a bank is "not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account").
203. *See Carpenter*, 137 S. Ct. at 2220.

modern society.[204] Indeed, many bioethicists have specifically criticized DTC providers for propagating the notion that the "democratization" of genetics is key to "self-actualization" in order to further their economic aims of biobanking genetic information.[205] Moreover, the bioethicist Dr. Sandra Soo-Jin Lee, in conducting a study of eighty individuals who had undergone genetic testing via 23andMe, found that information regarding medical propensities revealed by genetic tests had little impact on their medical decisions and lifestyle choices.[206]

Although Dr. Lee's study is more anecdotal than comprehensive, it strongly supports the notion that acquiring one's genetic information from a DTC provider is not fundamental to identity formation or social relationships in the modern age. In addition, even if genetic tests are construed as a social or personal necessity, there are clinical genetic tests performed by physicians that provide comprehensive screening and are subject to more stringent privacy rules.[207] Consumers may seek out such clinical tests (albeit at a higher cost) if they are uncomfortable with DTC providers' privacy terms. Thus, unlike an individual transacting with a cell phone provider, voluntary assumption of risk of exposure to law enforcement through transacting in genetic data with a DTC provider could be presumed in this context.

2. *Carpenter*'s Consideration of Depth and Comprehensive Reach of DTC Genetic Databases Is Immaterial

Warrantless searches of DTC genetic testing databases by law enforcement may be justifiable under the third-party doctrine on the basis of assumption of risk alone. Nonetheless, compelling arguments would have to be presented as to why, pursuant to *Carpenter*, genetic information is not subject to constitutional protections given its depth and comprehensive reach.

There is, however, a considerable body of jurisprudence that supports the notion that there should not be an exception for genetic information that is validly subject to a warrantless search under the third-party doctrine and the Fourth Amendment.[208] In addition, Justice Gorsuch has asserted that balancing the abstract "value of privacy in a particular setting" with "society's interest in combating crime" is a policy inquiry best left to an elected legislature to decide.[209] The following sections evaluate *Carpenter*'s consideration of depth and comprehensive reach as applied to disclosed genetic information through the lens of these criticisms.

---

204. *See, e.g.*, Kaitlyn Greenidge, Opinion, *The Family History DNA Can't Reveal*, N.Y. TIMES (Dec. 15, 2018), https://www.nytimes.com/2018/12/15/opinion/sunday/dna-ancestry-test.html [https://perma.cc/Z4WY-DBKP].

205. Sandra Soo-Jin Lee, *American DNA: The Politics of Potentiality in a Genomic Age*, 54 CURRENT ANTHROPOLOGY S77, S85 (2013); *see also* Greenidge, *supra* note 204.

206. *See* Lee, *supra* note 205, at S79–S80.

207. *See* Ram, *supra* note 76, at 889. Physicians constitute health-care providers and are therefore subject to HIPAA's privacy rules. *See supra* note 90 and accompanying text.

208. *See infra* Part III.B.2.a.

209. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2265 (2018) (Gorsuch, J., dissenting).

a. Depth of Information

As stated above, the "depth" prong under *Carpenter* considers whether the nature of the disclosed information is "deeply revealing" and, accordingly, protected as "private" under the Constitution.[210]

The nature of genetic information is such that it has the ability to reveal a wide scope of information about a consumer's ethnicity, medical background, and familial relationships.[211] However, DNA samples legally acquired by the police as part of routine investigations likewise can reveal intimate information of this nature.[212] Nonetheless, as of yet, the judiciary has not considered such DNA samples to be protected under the Fourth Amendment merely by virtue of their potential to disclose "private" information beyond what is needed for identification of a suspect.

In *California v. Greenwood*,[213] the Court held that an individual has no reasonable expectation of privacy in property abandoned in a public space that is accessible to law enforcement.[214] Pursuant to *Greenwood*, several state courts have held that where an individual voluntarily "abandons" a biological sample containing DNA in a public place, he or she can claim no reasonable expectation of privacy in the biological sample.[215] As the Washington Supreme Court explicitly stated in *State v. Athan*,[216] "There is no subjective expectation of privacy in discarded genetic material."[217] Rather, if a DNA sample is abandoned or "knowingly exposed" to public view, the Fourth Amendment does not protect that sample from search or seizure by law enforcement.[218] Similarly, if the Informant knowingly assumes the risk of exposure of his or her genetic information to law enforcement, this act is, arguably, functionally equivalent to abandoning that genetic information in a public space accessible to law enforcement. Accordingly, *Greenwood* and its state law progeny suggest that genetic information disclosed to third-party DTC providers may not be entitled to any special constitutional protections as "genetic material."

In addition, it is highly unlikely that law enforcement would retain and misuse such genetic material given the purpose of genetic searches by law enforcement and potential legislative constraints on abuse. First, the Court has held that collected DNA samples that may reveal intimate information are not inherently entitled to Fourth Amendment protections because law

210. *See id*. at 2217, 2223 (majority opinion); *see also supra* Part II.B.2.
211. *See supra* Part I.B.2.
212. *See supra* note 56 and accompanying text.
213. 486 U.S. 35 (1988).
214. *See id.* at 40–41.
215. *See, e.g.*, State v. Wickline, 440 N.W.2d 249, 252–53 (Neb. 1989) (involving saliva from a discarded cigarette butt); People v. Ayler, No. 3217/2003, 2004 WL 2715317, at *5 (N.Y. Sup. Ct. Sept. 22, 2004) (same); State v. Athan, 158 P.3d 27, 33–34 (Wash. 2007) (en banc) (involving saliva from an envelope).
216. 158 P.3d 27 (Wash. 2007) (en banc).
217. *Id.* at 37.
218. *See* Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U. L. REV. 857, 863 (2006); *see also* Pike, *supra* note 28, at 2000.

enforcement merely tests the sample for the thirteen loci that are relevant to identification.[219] As the Third Circuit held in *United States v. Mitchell*,[220] the fear of "hypothetical abuse"[221] by law enforcement of the "sensitive information that can be mined from a person's DNA" should not exclusively govern the analysis of whether the information is protected under the Fourth Amendment.[222] Instead, particularly where there are legislative constraints preventing abusive use of DNA samples, law enforcement's legitimate interest in using DNA to identify suspects in crimes should be accorded equal weight in the analysis.[223]

Similarly, law enforcement requests for genetic information from DTC providers would likely be limited to information which is necessary for identification of the putative suspect: the names of the familial matches to the suspect genetic profile.[224] There are no state or federal statutes explicitly regulating the use of genetic information obtained in the course of an investigation.[225] Nonetheless, a patchwork of private and legislative solutions could likely prevent either access to more sensitive genetic information or potential abuse of such information should law enforcement be granted access.

DTC providers likely would resist releasing more sensitive genetic information from their databases to law enforcement because doing so would jeopardize consumer trust in their services.[226] Indeed, Ancestry's resistance to disclosing the genetic information of one of its users in 2014 serves as powerful anecdotal evidence of how a DTC provider would likely react to a subpoena for genetic information.[227] There, Ancestry refused to even provide law enforcement with the name of an individual whose genetic information was stored within its databases until it was compelled to do so by court order.[228]

Third-party providers like Ancestry and 23andMe may, in fact, be well-positioned to resist and narrow law enforcement requests for information in court.[229] Even if third-party providers have no meaningful grounds to reject a government subpoena pursuant the third-party doctrine, such providers have, on occasion, successfully obtained court orders limiting the scope of information required by the subpoena in order to protect the privacy interests

219. *See* Maryland v. King, 569 U.S. 435, 464–65 (2013); *see also*, *e.g.*, Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 658 (1995) (holding that drug testing students was appropriate because the "tests at issue here look only for drugs, and not for whether the student is, for example, epileptic, pregnant, or diabetic").

220. 652 F.3d 387 (3d Cir. 2011).

221. *Id.* at 407 (quoting United States v. Weikert, 504 F.3d 1, 13 (1st Cir. 2007)).

222. *Id.* (quoting United States v. Amerson, 483 F.3d 73, 85 (2d Cir. 2007)).

223. *See King*, 569 U.S. at 464–65; *see also Mitchell*, 652 F.3d at 407–08.

224. *See supra* Parts I.B.3–4.

225. *See supra* Part I.B.3.

226. Pike, *supra* note 28, at 1987.

227. *See supra* notes 105–08 and accompanying text.

228. *See supra* notes 105–08 and accompanying text.

229. Kerr, *supra* note 131, at 598–99.

of their consumers.[230] Therefore, DTC providers are strongly incentivized, and likely have sufficient legal grounds, to petition courts to narrow law enforcement requests for sensitive genetic information to, at most, disclosure of the names of potential Informants.

Legislative efforts like HIPAA and GINA also suggest that the federal legislature is finely attuned to the risks of abusive uses of genetic information.[231] Even if there are not existing restrictions on law enforcement requests for genetic information stored by DTC providers,[232] these legislative efforts suggest that Congress is capable of and willing to act if any abusive uses of genetic information by law enforcement were to come to light.

Finally, investigations of genetic databases have measurable benefits to law enforcement and society at large. From the perspective of corrective justice, identifying perpetrators of crimes allows for punishment of the wrongdoer and "provides peace and resolution to the victims and their families."[233] In addition, such investigations allow law enforcement to identify suspects in particularly heinous or violent unsolved crimes for the benefit of public safety, which, in turn, reinforces public trust in the criminal justice system.[234] The judiciary, therefore, might be hesitant to preemptively limit this beneficial law enforcement practice when the risk of excessive surveillance of genetic material is merely speculative in nature and may not materialize.

b. Comprehensive Reach

The reach of DTC genetic databases is undoubtedly extensive, as the genetic material of over fifteen million consumers is housed in these databases.[235] Furthermore, the genetic material of those fifteen million individuals has the potential to implicate tens of millions of additional individuals who share genetic material with the databased individuals.[236] Pursuant to *Carpenter*, allowing law enforcement to conduct investigations

230. In 2006, for example, after the U.S. Department of Justice (DOJ) issued an expansive subpoena to Google for records of user queries, Google convinced a district court in the Northern District of California to narrow the subpoena. *See* Gonzales v. Google, Inc., 234 F.R.D. 674, 683–84 (N.D. Cal. 2006). Google argued that complying with the subpoena imposed an undue burden because it risked eroding user's trust in their services. *Id.*; *see also* Kerr, *supra* note 131, at 598–99. The district court judge noted that the subpoena, which requested that records of any queries made by Google's users during a two-month window be made available to the DOJ, risked revealing extraordinarily private searches made by Google's users, such as searches for an abortion clinic or sexually explicit materials. *See Gonzales*, 234 F.R.D. at 687. The judge therefore required that the DOJ narrow its subpoena in order to better protect the privacy interests of Google's users. *See* Kerr, *supra* note 131, at 599.

231. *See supra* notes 87–93 and accompanying text.

232. *See supra* notes 87–93 and accompanying text.

233. Suter, *supra* note 38, at 375.

234. *See* Maryland v. King, 569 U.S. 435, 442 (2013); *see also* Amitai Etzioni, *DNA Tests and Databases in Criminal Justice: Individual Rights and the Common Good*, *in* DNA AND THE CRIMINAL JUSTICE SYSTEM: THE TECHNOLOGY OF JUSTICE 197, 200–01 (David Lazer ed., 2004).

235. *See supra* Part II.B.1.

236. *See supra* Part I.B.4.

of the genetic material of millions of individuals without individualized suspicion might constitute prohibited "suspicionless searches" under the Fourth Amendment.[237]

Notably, however, CODIS is similar in scope, as it has approximately seventeen million offender profiles within its databases.[238] The comprehensive breadth of CODIS is justified on the grounds that arrestees and felons have diminished expectations of privacy as a result of their criminal history and because there is a measurable possibility that arrestees and felons will reoffend.[239] Nonetheless, the law enforcement practice of identifying suspects in CODIS through partial matches to offender profiles or familial searches similarly implicates a much wider web of presumably "innocent" individuals who maintain reasonable expectations of privacy.[240] In the absence of uniform agreement among state legislatures about the permissibility of long-range familial searches,[241] it may not be appropriate for the judiciary to issue broad, sweeping policy judgments as to whether such searches on DTC genetic databases implicate too many individuals or risk suspicionless searches.[242]

Indeed, many individuals likely support law enforcement's use of DTC genetic databases to solve cold cases. In a recent survey by four scholars at the Center for Medical Ethics and Health Policy at Baylor College of Medicine that was circulated to 1587 individuals, 79 percent of respondents "supported police searches of genetic websites that identify genetic relatives," and 62 percent of respondents supported the "disclosure of DTC genetic testing customer information to police" as a means of identifying suspects in violent crimes.[243]

Furthermore, the use of DTC genetic databases as a means of identifying suspects may balance some of the extreme racial disparities present in the criminal justice system and CODIS.[244] People of color likely have disproportionate representation in CODIS as a result of inherent racial biases in arrests and sentencing in the criminal justice system.[245] By contrast, DTC providers' databases are disproportionality skewed toward white individuals of European descent.[246] Consequently, permitting law enforcement's investigation of DTC genetic databases to identify suspects may "begin to

237. *See supra* Part II.B.2.b.

238. *See supra* note 48 and accompanying text.

239. *See* United States v. Kincade, 379 F.3d 813, 838–39 (9th Cir. 2004); *see also* Murphy, *supra* note 41, at 317.

240. *See supra* Part I.A.3.

241. *See supra* Part I.A.3.

242. *See supra* note 209 and accompanying text.

243. Christi J. Guerrini et al., *Should Police Have Access to Genetic Genealogy Databases? Capturing the Golden State Killer and Other Criminals Using a Controversial New Forensic Technique*, PLOS BIOLOGY, Oct. 2, 2018, at 1, 3, https://journals.plos.org/plosbiology/article/file?id=10.1371/journal.pbio.2006906&type=printable [https://perma.cc/VC8J-X4MY].

244. Ram et al., *supra* note 90, at 1078.

245. *See* KRIMSKY & SIMONCELLI, *supra* note 49, at 253–56.

246. *See supra* Part I.B.1.

redress, in at least in one respect, disparities in the criminal justice system."[247]

Given these countervailing policy interests, it may be more prudent to allow elected state or federal legislatures to gauge public interest regarding the comprehensive reach afforded by law enforcement conducting long-range familial searches on DTC genetic databases and, if necessary, enact statutes limiting this reach.[248]

3. Third-Party DTC Providers Maintain Proprietary Interests in Stored Genetic Information

Finally, law enforcement searches of DTC genetic databases may be justified on the grounds that the Informant maintains no reasonable expectation of privacy based on proprietary interests in the genetic information. Under this perspective, the Informant relinquishes her proprietary interests in the genetic information by granting the DTC provider possession and use of her biological sample and genetic information.

Although the privacy policies of DTC providers like 23andMe and Ancestry claim in their terms of use and privacy policies that Informants maintain "ownership" over their genetic information,[249] these statements may be viewed with a healthy dose of skepticism. Because the DTC providers typically reserve an exclusive license to use and distribute their consumers' genetic information in their terms of service, many reporters and legal experts have suggested that ownership rights in the genetic information are granted to DTC providers by consumers in spite of this purported waiver of such rights.[250]

A license, traditionally construed, functions merely as a permissive contract to use another's property for a particular purpose.[251] However, a more modern conception of licensing and its function in modern transactions suggests that exclusive licenses may, in effect, transfer certain divisible property rights in information and therefore serve "the same commercial

247. Ram et al., *supra* note 90, at 1079.

248. For example, some legal scholars have suggested a genetic equivalent to the Stored Communications Act, which would "ensure that the government cannot subject ordinary individuals to suspicionless genetic searches, while allowing investigators to access genetic data where there is reason to believe a particular individual may be tied to a particular crime." *Id.*

249. *See supra* Part I.B.3.a.

250. *See* Joel Winston, *Ancestry.com Takes DNA Ownership Rights from Customers and Their Relatives*, THINKPROGRESS (May 17, 2017, 7:54 PM), https://thinkprogress.org/ancestry-com-takes-dna-ownership-rights-from-customers-and-their-relatives-dbafeed02b9e [https://perma.cc/6TUB-ZVWK]; *see also* Jacob Brogan, *Who Owns Your Genetic Data After a Home DNA Test*, SLATE (May 23, 2017, 8:23 PM), https://slate.com/technology/2017/05/ancestrydnas-terms-and-conditions-sparked-a-debate-about-ownership-of-genetic-material.html [https://perma.cc/V625-T7GS].

251. *See License*, BLACK'S LAW DICTIONARY (10th ed. 2014).

purpose as an assignment."[252] Likewise, in the realm of patent law, where a purported license transfers "substantially all" of the licensors rights to use and sell patented inventions, courts have considered the transfer an assignment.[253]

Under copyright law, the prevailing view suggests that an exclusive license to use a party's information does not effectuate a transfer of copyright ownership under the Copyright Act of 1976.[254] Nevertheless, there is a countervailing minority view that an exclusive license "constitutes a transfer of copyright ownership" in information under the Copyright Act.[255] Furthermore, where a party grants itself "sublicensing" rights as part of the "licensing" agreements, some courts have treated the agreement as an assignment under the Copyright Act.[256]

Thus, although 23andMe and Ancestry allege that their interest in consumers' genetic information is only a "license" to use such information, a comprehensive investigation of the rights associated with those licenses might support notion that they are, in practice, an assignment of property rights. The licenses grant the companies expansive permission to use their consumers' genetic information, as well as the capacity to sublicense the information without the explicit permission of the consumer.[257] Moreover, 23andMe grants itself an "irrevocable" exclusive license—a license which one scholar has argued is better construed as a "deed" conveying an ownership interest.[258]

The nature of these licenses undercuts the DTC providers' claims that no proprietary rights in genetic information are transferred from the Informant. Justice Kennedy suggested that a proprietary interest in information is transferred to the third party where the Informant fails to maintain possession of or use the information as a result of the transaction.[259] The granted licenses, therefore, could support the argument that such a proprietary interest is conveyed and that transacting in genetic information with DTC providers should not be understood as merely a "bailment" of property to the third-party genetic testing provider.

---

252. 1 RAYMOND T. NIMMER & JEFF C. DODD, MODERN LICENSING LAW § 1:11 (2018); *see also* Christopher M. Newman, *An Exclusive License Is Not an Assignment: Disentangling Divisibility and Transferability of Ownership in Copyright*, 74 LA. L. REV. 59, 61 (2013).

253. *See* CMS Indus. v. L. P. S. Int'l, Ltd., 643 F.2d 289, 294 (5th Cir. Unit B Apr. 1981).

254. Pub. L. No. 94-553, 90 Stat. 2541 (codified as amended in 17 U.S.C.); *see also* Gardner v. Nike, Inc., 279 F.3d 774, 779 (9th Cir. 2002).

255. Traicoff v. Dig. Media, Inc., 439 F. Supp. 2d 872, 877–78 (S.D. Ind. 2006); *see also In re* Golden Books Family Entm't, Inc., 269 B.R. 311, 314 (Bankr. D. Del. 2001); 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 10.02 (2018).

256. *See In re* XMH Corp., 647 F.3d 690, 696 (7th Cir. 2011).

257. *See supra* Part I.B.3.b.

258. Christopher M. Newman, *A License Is Not a "Contract Not to Sue": Disentangling Property and Contract in the Law of Copyright Licenses*, 98 IOWA L. REV. 1101, 1110, 1115 (2013).

259. *See* Carpenter v. United States, 138 S. Ct. 2206, 2224, 2228 (2018) (Kennedy, J., dissenting).

In addition, Jorge Contreras, an expert in intellectual property law and human genetics, has presented strong policy arguments against exclusively vesting property rights to genetic information in those to whom the genetic material belongs.[260] Professor Contreras asserts that granting "property-like rights" to research participants in their transferred genetic material, and any inventions derived from that material, risks "creat[ing] an anticommons of significant proportions" that would stymy important biomedical research on the human genome.[261] Similarly, requiring "propertized consent" for the use of genetic information from potentially "millions" of individuals is not feasible in practice and would likewise hinder important genetic research.[262] Indeed, courts have been reluctant to allow individuals to claim property rights in patented scientific inventions derived from their cells.[263]

In sum, under this perspective, the judiciary should not declare that: (1) the Informant maintains an unconditional property interest in their genetic information despite the "license" agreement; or (2) that "generational consent" from the Collective is necessary to transfer property rights in genetic material to the third-party DTC provider because of the dramatic ramifications such a holding might have on the field of biomedical research.

C. The Third-Party Doctrine as Inapplicable to Genetic Information: Protection of Consumers' Genetic Information

Opponents of warrantless law enforcement searches of DTC providers' databases would, by contrast, assert that the third-party doctrine does not apply because genetic information is entitled to special protections under the Fourth Amendment and the broader confines of the Constitution.

While the assumption-of-risk theory underlying the third-party doctrine could be inapplicable in the context of transacting with a DTC provider, the comprehensive reach and breadth of genetic information stored by DTC providers may justify its exclusion from the third-party doctrine pursuant to *Carpenter*. Alternatively, some might argue that Informants maintain a proprietary interest in their genetic information despite disclosure to a third-party provider.

1. No Voluntary Assumption of Risk by Consumers

The premise that individuals "voluntarily" assume the risk of the exposure to law enforcement under the third-party doctrine may be compromised by a probable lack of understanding concerning this risk. As Justice Thurgood Marshall argued in his dissent in *Smith*, "[p]rivacy is not a discrete commodity, possessed absolutely or not at all," and often when "we disclose certain facts to a bank or phone company for a limited business purpose [we do not] assume that this information will be released to other persons for

260. *See generally* Jorge L. Contreras, *Genetic Property*, 105 GEO. L.J. 1 (2016).
261. *See id.* at 36.
262. *See id.*
263. *See, e.g.*, Moore v. Regents of Univ. of Cal., 793 P.2d 479, 492 (Cal. 1990).

other purposes."[264] Therefore, voluntary assumption of risk perhaps cannot be presumed where a consumer reasonably believes that the third-party business has exclusive access to his or her information and will use it for a limited business purpose.[265]

Indeed, it is not clear that the Informant, in disclosing his or her genetic information to a DTC provider, understands the attendant risks that law enforcement can (1) identify a relative as a suspect using that information; and (2) potentially store the Informant's unique genetic information derived from an investigation for an indefinite amount of time for alternative uses.[266] The Informant likely does not understand this risk because the terms of use and privacy policies of DTC providers imply that his or her data is subject to a high degree of confidentiality.[267] DTC providers' terms suggest that a consumer's genetic information will not be shared with any external parties without the informed consent of that consumer.[268] Furthermore, even where the genetic information is shared with partners of the DTC provider, the providers state that data will be anonymized.[269] It is therefore unlikely that the Informant voluntarily consents to the implicit risk that the DTC provider, or one of its labs, research partners, or business partners, may subsequently hand over the Informant's genetic information to law enforcement.

In addition, the claim that the Informant explicitly assumes the risk posed by law enforcement investigations by consenting to the terms of use and privacy policies that acknowledge this risk likely misconstrues consumers' interactions with these contracts of adhesion. The Second Circuit has held that the "[c]larity and conspicuousness of . . . terms are important in securing informed assent."[270] Even where the consumer is provided with notice of terms and asked to agree to them, if the terms are then buried within a linked,

264. *See* Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting). Justice Sotomayor has likewise argued that the scope of understanding regarding government access is relevant, stating, "I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on." United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

265. Justice William Brennan, Jr. strongly asserted this point in his dissent in *Miller*, explaining that "[a] bank customer's reasonable expectation is that, absent compulsion by legal process, the matters he reveals to the bank will be utilized by the bank only for internal banking purposes." United States v. Miller, 425 U.S. 435, 449 (1976) (Brennan, J., dissenting).

266. *See* Pike, *supra* note 28, at 2009–10.

267. *See supra* note 99 and accompanying text; *see also* Carpenter v. United States, 138 S. Ct. 2206, 2262–63 (2018) (Gorsuch, J., dissenting) ("Today we use the Internet to do most everything. . . . People often *do* reasonably expect that information they entrust to third parties, especially information subject to confidentiality agreements, will be kept private.").

268. *See supra* note 98 and accompanying text.

269. *See supra* note 99 and accompanying text. Although there is evidence that deidentified genetic information can be deanonymized with relative ease, the companies' terms of use and privacy policies do not explain this risk, and it is likely unfair to assume that the average layperson is aware of it.

270. Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 30 (2d Cir. 2002).

long, scrollable document which does not call attention to the provision at issue, informed assent may not be presumed.[271]

The provisions regarding law enforcement access to consumers' genetic information may be construed as "buried" within DTC provider's privacy policies and terms of use. For example, between 23andMe's privacy policy, terms of use, and informed-consent form, a consumer likely has to read through over fifty pages of documents to understand the full scope of his or her privacy rights.[272] The consent to law enforcement access in the terms of service is nestled in a long paragraph approximately ten pages into the document.[273] In the privacy statement, the reader must wade through approximately sixteen pages of documents to find the provision giving notice of potential disclosure of genetic information to law enforcement.[274] As the bioethicist Kayte Spector-Bagdady has noted, "[t]ransparency . . . is not the same thing as informed consent" when it comes to DTC provider's privacy policies and terms of use.[275] Because the provisions concerning law enforcement access are not obvious to an Informant faced with reading expansive privacy policies and terms of use, consent to, and thereby voluntary assumption of, the risk on the part of the Informant may not be established.

Moreover, regardless of the Informant's voluntary assumption of risk, the Target certainly has not similarly assumed the risk of exposure of his or her shared genetic material to law enforcement. Genetic information implicates a wide scope of related family members with overlapping genetic material. Thus, when the Informant discloses genetic information to a third party, the Informant has also, in effect, disclosed the genetic information of a number of relatives. The Target, however, likely has no idea that portions of his or her genetic code are held by a third-party provider or that this could ultimately lead to his or her arrest for a crime.[276] Indeed, for this reason, some medical ethicists have suggested that "generational consent" between all relatives who might be implicated by genetic information stored in DTC genetic databases should be required before disclosure.[277] Accordingly, there are strong arguments that the Target should likewise have voluntarily

271. *Id.* at 30–31; *see, e.g.*, Nguyen v. Barnes & Noble Inc., 763 F.3d 1171, 1177–79 (9th Cir. 2014) (considering conspicuousness and notice in the context of a website's terms of use).

272. The approximate page numbers for the following documents were derived through copying and pasting the text of each 23andMe policy statement into a word processing computer program.

273. *Terms of Service*, *supra* note 94.

274. *Privacy Highlights*, *supra* note 77.

275. Michael Schulson, *Spit and Take*, SLATE (Dec. 29, 2017, 12:04 PM), http://www.slate.com/articles/technology/future_tense/2017/12/direct_to_consumer_genetic_testing_has_tons_of_privacy_issues_why_is_the.html [https://perma.cc/5Q2B-SDCE].

276. *See* Molteni, *supra* note 9.

277. Susan E. Wallace et al., *Family Tree and Ancestry Inference: Is There a Need for a 'Generational' Consent?*, BMC MEDICAL ETHICS, Dec. 9, 2015, at 1, 7–8, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4673846/pdf/12910_2015_Article_80.pdf [https://perma.cc/XX4R-RETW].

assumed the risk under the third-party doctrine when it comes to shared genetic information.

2. *Carpenter* Justifies Excluding DTC Genetic Databases from the Third-Party Doctrine

Opponents of warrantless law enforcement searches of DTC genetic databases could argue that the depth and comprehensive reach of the genetic information available in DTC genetic databases weigh against the application of the third-party doctrine pursuant to *Carpenter*. This section discusses the specific privacy risks associated with the depth and comprehensive reach of private genetic databases in greater detail.

a. Depth of Information

Genetic information provides an exceptionally intimate window into the Informant's personhood, medical health, and familial relationships.[278] At first blush, jurisprudence concerning samples of DNA that are abandoned in public or housed in CODIS's databases might suggest that, despite its exceptional qualities, genetic information does not merit special privacy protections where it is validly obtained for a limited purpose.[279] However, upon a more exacting inquiry, searching for genetic information on DTC genetic databases may, in fact, be factually distinct from collecting abandoned DNA or testing a DNA sample in CODIS.

Although the DNA abandonment cases strongly suggest that there are no special privacy protections afforded to individuals whose DNA is validly acquired by the police,[280] drawing an analogy between the abandonment of DNA and entrustment of genetic information to a third party is likely unwarranted. Discarding a cigarette, cup, or other object that contains an individual's DNA constitutes a total, voluntary abandonment of expectations of privacy in that object and, by extension, the DNA sample left on that object.[281] These instances stand in stark contrast to entrusting one's genetic information to a DTC provider who promises to keep it private.[282] When an individual entrusts information to a third party in this capacity, his or her expectation of privacy in the information is merely diminished or reduced.[283] As the Court held in *Carpenter*, where privacy interests are merely reduced, a more comprehensive analysis of the nature of the privacy interest in the information is appropriate for the Fourth Amendment search analysis.[284]

---

278. *See* Pike, *supra* note 28, at 1985; *see also* Part I.B.3.
279. *See supra* notes 215–16.
280. *See supra* note 215 and accompanying text.
281. *See, e.g.*, State v. Athan, 158 P.3d 27, 37 (Wash. 2007) (en banc) (holding that "voluntary relinquishment of a bodily fluid" is functionally equivalent to leaving behind "fingerprints, footprints, or other possibly incriminating evidence").
282. *See supra* Part I.B.3.b.
283. *See supra* Part II.B.2.
284. *See* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

In *Maryland v. King*,[285] the Court specified that entering the STR testing of DNA samples into CODIS did not implicate the privacy interests of the tested individual because STR loci "do not reveal . . . genetic traits."[286] As Erin Murphy, an expert in forensic DNA typing, has stated, *King* therefore makes clear that "unfettered access to the entire genome of an individual should not be presumed from the cases approving forensic databasing."[287] The Court in *King* failed to elaborate upon why "genetic traits" would trigger more extensive privacy interests; however, other legal scholarship and cases elaborate upon this point.

First, genetic information provided to DTC providers may reveal the Informant's genetic propensity for certain medical conditions or diseases.[288] In *Skinner v. Railway Labor Executives' Ass'n*,[289] the Court held that testing urine could reveal "private medical facts" and therefore constituted a search under the Fourth Amendment, even though urine testing does not involve a bodily intrusion.[290] This holding implies that individuals maintain a reasonable expectation of privacy regarding their medical history and other private medical information.[291]

Second, genetic information given to DTC providers reveals detailed information about the Informant's familial ties, thereby implicating his or her familial privacy. The results provided to law enforcement from a search of a suspect's profile in DTC providers' databases likely include a long list of related individuals who have submitted their genetic information to the provider for testing.[292] Law enforcement, in the course of building family trees and investigating potential suspects, may inadvertently reveal unknown familial relationships.[293] This may impact both the Informant's intimate conceptions of his familial identity and the familial identity of the Collective.[294] *Carpenter* clearly indicates that individuals maintain a reasonable expectation of privacy in familial associations under the Fourth Amendment.[295] Furthermore, there is a long constitutional history of protecting familial decision-making and integrity from government surveillance or intrusion.[296] There are, therefore, strong privacy interests in both the medical and familial information revealed by genetic testing, which

285. 569 U.S. 435 (2013).
286. *Id.* at 464.
287. Murphy, *supra* note 41, at 316.
288. *See supra* Part I.B.2.
289. 489 U.S. 602 (1989).
290. *Id.* at 617.
291. *See id.*; *see also* United States v. Kincade, 379 F.3d 813, 850 (9th Cir. 2004) (Reinhardt, J., dissenting) (stating that DNA is entitled to Fourth Amendment protection because "analysis can reveal the presence of traits for thousands of known diseases, and countless numbers of diseases which are currently unknown"); Raynor v. State, 99 A.3d 753, 771–72 (Md. 2014) (Adkins, J., dissenting).
292. *See supra* note 80 and accompanying text.
293. *See* Suter, *supra* note 38, at 311–12.
294. *See id.* at 347–48.
295. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).
296. *See* Suter, *supra* note 38, at 363–64; *see also supra* note 159 and accompanying text.

suggest that law enforcement's unfettered access to this information under the third-party doctrine would be inappropriate.

However, as is the case with testing DNA samples and entering them into CODIS, law enforcement's interest in genetic information disclosed to DTC providers is limited to its ability to identify a suspect. *King* and *Mitchell* lend support to the understanding that the risks of law enforcement requesting a broader scope of more intimate genetic information from DTC genetic databases are unlikely to come to fruition and do not justify excluding genetic information from valid law enforcement investigation.[297] However, both of these holdings were issued in the face of preexisting legislative restrictions limiting the use of genetic information in DNA databases. In *Mitchell*, the Third Circuit held that the possibility of abuse of private information derived from DNA was negligible because federal law[298] imposes criminal penalties for misuse of biological samples or DNA results obtained from samples in CODIS.[299] Similarly, in *King*, the Court noted that the risk that an individual's expectation of privacy in their genetic traits would be invaded were minimal because a Maryland statute provided that only DNA records that "directly relate to the identification of individuals [could] be collected and stored" in the state's DNA database.[300]

By contrast, there are no explicit legislative constraints on either the depth of genetic information that law enforcement can collect from DTC genetic databases or law enforcement's retention and future use of such genetic information.[301] The possibility that the legislature would be able to react in a timely fashion if law enforcement began collecting and misusing sensitive genetic information is a thin reed on which to rest. In addition, relying on DTC providers to regulate law enforcement requests is not a foolproof protection.[302] As Daniel Solove has pointed out, third-party providers are often inclined to disclose consumer information to law enforcement "in times of crisis or when serious crimes are at issue."[303]

Without meaningful restrictions on law enforcement's retention and use of genetic information obtained from DTC genetic databases, there is a sizable risk of abuse of that information. Historically, where the government has been granted access to certain forms of information with limited regulatory oversight, it has used that information for purposes beyond its intended scope.[304] In collecting data from third-party businesses, law enforcement officers typically cannot pinpoint in advance what particular information

297. *See supra* Part III.B.2.a.

298. 42 U.S.C. § 14135a(a)(1)–(2) (2012).

299. *See* United States v. Mitchell, 652 F.3d 387, 407 (3d Cir. 2011).

300. Maryland v. King, 569 U.S. 435, 465 (2013) (quoting MD. CODE ANN., PUB. SAFETY § 2-505(b)(1)).

301. *See supra* Part I.B.3.

302. *See* United States v. White, 401 U.S. 745, 793 (1971) (Harlan, J., dissenting); *see also* Solove, *supra* note 165, at 1098.

303. Solove, *supra* note 165, at 1098.

304. *See* Joh, *supra* note 218, at 879; *see also* Barry Steinhardt, *Privacy and Forensic DNA Data Banks*, *in* DNA AND THE CRIMINAL JUSTICE SYSTEM: THE TECHNOLOGY OF JUSTICE, *supra* note 234, at 173, 174.

contained within that data is directly relevant to its criminal investigations.[305] Information requests for third-party data by law enforcement are consequently relatively broad in scope and inevitably sweep up intimate details beyond the information specifically needed to identify the suspect in a particular crime.[306] Without clear regulations or policies on retention or use of individuals' intimate information, the government and law enforcement could later use that information to target political undesirables.[307] While the possibility of such misuse may seem remote, at various points throughout the latter half of the of twentieth century, the FBI, the CIA, Congress, and the U.S. Army have collected intimate information from U.S. citizens for the purposes of identifying and monitoring political dissidents.[308]

If law enforcement and the government begin to build their own genetic database using information gleaned from DTC genetic databases, the risks of misuse associated with such data are troubling.[309] Specifically, such a database would increase the possibility of the resurgence of state-sponsored genetic discrimination.[310] The potential for genetic discrimination based on genetic medical propensities has, to some extent, been capped by GINA.[311] However, the ethnographic and behavioral genetic traits revealed by DTC genetic tests could certainly be misused in a discriminatory fashion. For example, scientists have recently identified an alarming trend of white nationalists linking academic papers on genetic propensities among certain ethnographic groups with ill-informed claims of white supremacy.[312] While perhaps there are sufficient legal and political safeguards to prevent state-sponsored racial genetic discrimination of the kind advocated for by white supremacists, these circumstances suggest that the belief that behavioral genetic traits are indicative of actual human behavior remains powerful in contemporary society.

Indeed, as recently as the 1990s, scientists have attempted to discover a "crime gene" that could justify surveillance or control of individuals deemed to be "genetically predisposed to criminality."[313] Erin Murphy has warned that these attempts to identify genetic indicia of criminality could be renewed and expanded for use in the criminal justice system as certain behavioral and cognitive traits could be linked to deviant or violent behavior.[314] Murphy asserts that the criminal justice system could easily slot studies on genetic

305. Riley v. California, 134 S. Ct. 2473, 2492 (2014).
306. *See id.*
307. *See* Solove, *supra* note 165, at 1102.
308. See *id.* at 1107–08 for a comprehensive list of such instances.
309. Ram, *supra* note 76, at 894.
310. Steinhardt, *supra* note 304, at 174.
311. *See supra* note 92 and accompanying text.
312. *See* Amy Harmon, *Why White Supremacists Are Chugging Milk (and Why Geneticists Are Alarmed)*, N.Y. TIMES (Oct. 17, 2018), https://www.nytimes.com/2018/10/17/us/white-supremacists-science-dna.html [https://perma.cc/7F4Z-XPEE]; *see also ASHG Denounces Attempts to Link Genetics and Racial Supremacy*, 103 AM. J. HUM. GENETICS 636, 636 (2018).
313. Joh, *supra* note 218, at 876–77.
314. *See* MURPHY, *supra* note 40, at 227–28.

predispositions into, for example, the surveys that evaluate a criminal's likelihood of recidivism based on social and economic factors.[315]

The potential that "genetic predeterminism" could justify greater surveillance of particular individuals therefore may warrant protecting genetic information from unregulated access by law enforcement.[316] Furthermore, it is clear that genetic information can reveal constitutionally protected private information. Accordingly, the depth of information available in DTC genetic databases provides a strong basis for the argument that the third-party doctrine does not apply and any investigations of such databases must comply with the Fourth Amendment.

b. Comprehensive Reach of DTC Genetic Databases

In addition, the comprehensive breadth of DTC genetic databases could suggest that law enforcement should not be entitled to conduct suspicionless searches of those databases.[317] While DTC genetic databases are currently similar in breadth to CODIS, the size of CODIS is premised on a "legitimate government interest" in monitoring arrestees and convicts.[318] Specifically, the inclusion of millions of arrestees and convicts in a national DNA database has been justified on the grounds that there is a quantifiable possibility that arrestees and convicts will reoffend.[319] Furthermore, the government interest is deemed more weighty than the privacy interests of arrestees and convicts because a convicted felon or arrestee has diminished expectations of privacy.[320] Indeed, the Court in *King* took pains to distinguish searches on CODIS from "programmatic searches of . . . the public at large," which are prohibited in the "absence of individualized suspicion."[321]

Law enforcement officials could attempt to frame programmatic searches of DTC genetic databases as a "legitimate government interest" because they help to identify suspects in sexual or violent crimes.[322] Regardless, it is difficult to imagine that a court would find a search of a database of over fifteen million citizens justifiable on the grounds that millions of individuals vacated any reasonable expectation of privacy by deciding to take a fifty dollar genetic test to find out whether they have ancestors from unexpected locations or a genetic predisposition to disliking the taste of broccoli.

Moreover, searches of DTC genetic databases implicate the genetic material of a comprehensive net of individuals beyond those consumers whose profiles are explicitly within the database. Indeed, the aforementioned study of long-range familial searches conducted on DTC genetic databases

315. *Id.*
316. *See supra* Part II.B.2.a.
317. *See supra* Part II.B.2.b.
318. *See* United States v. Kincade, 379 F.3d 813, 838–39 (9th Cir. 2004); *see also* Murphy, *supra* note 41, at 317.
319. Maryland v. King, 569 U.S. 435, 462–63 (2013).
320. *Id.*
321. *Id.*
322. *See, e.g.*, United States v. Salerno, 481 U.S. 739, 749 (1987) (holding that the government's interest in preventing crime by past arrestees is both legitimate and compelling).

estimated that only 2 percent of a target population would need to be on a DTC genetic database to find a third cousin or closer match to a suspect profile.[323] Assuming that the vast majority of individuals submitting their genetic information are U.S. citizens, approximately 4 to 5 percent of the U.S. population have disclosed their genetic information to DTC providers.[324] It is thus likely that DTC providers could implicate a majority of citizens within the United States. State legislatures and the FBI have either prohibited or imposed meaningful limits on the capacity of law enforcement to conduct similar programmatic searches for a family member of a suspect DNA profile on CODIS.[325] Although the consensus on what constitutes an appropriate familial search is not uniform, these limitations strongly suggest that the public is not comfortable with searches of innocent civilians by virtue of their familial relationship to a suspect.

Finally, while it is easier to justify law enforcement's need for an expansive database of genetic data to solve violent or sexual crimes, there is a serious risk that, without appropriate regulations, such databases could eventually be used by law enforcement to solve less serious crimes.[326] The vast expansion of qualifying crimes for inclusion in CODIS in the past two decades supports the probability that this will occur.[327]

Therefore, DTC genetic databases collectively may be construed as a universal database with an extremely comprehensive reach that, without regulation, would allow law enforcement to find suspects in any crime where a DNA sample was left behind. Arguably, a search of such databases is the quintessential search of millions of public citizens without individualized suspicion of wrongdoing that the Fourth Amendment is specifically designed to guard against.[328] As such, the comprehensive reach of DTC genetic databases strongly supports excluding warrantless searches of such databases from the third-party doctrine.

3. Ownership of Genetic Information Is Not Vested in Third-Party DTC Providers

Finally, opponents of warrantless searches of DTC genetic databases would likely maintain that the Informant reserves full proprietary interests in genetic information disclosed to a third-party DTC provider. The Informant could allege a subjective expectation of privacy in his or her genetic information given that the privacy policies and terms of use of DTC providers expressly state that they do not take ownership in their users' genetic

323. *See* Erlich et al., *supra* note 110, at 691; *see also* Carolyn Y. Johnson, *Even If You've Never Taken a DNA Test, a Distant Relative's Could Reveal Your Identity*, WASH. POST (Oct. 11, 2018), https://www.washingtonpost.com/science/2018/10/11/even-if-youve-never-taken-dna-test-distant-relatives-could-reveal-your-identity/ [https://perma.cc/Z43B-NB8Q].

324. *See supra* notes 66, 70 and accompanying text.

325. *See supra* Part I.A.3.

326. *See* Zhang, *supra* note 20.

327. *See* United States v. Kincade, 379 F.3d 813, 845 (9th Cir. 2004) (Reinhardt, J., dissenting).

328. *See supra* Part II.A.

information.[329] However, the opponent would have to prove that the Informant's subjective expectations of proprietary interests in the information are objectively reasonable in light of the Fourth Amendment's protections of property, the terms of the transaction with the third-party DTC providers, and relevant positive law.

From the outset, opponents could likely argue that the Informant has a special proprietary interest in information directly pertaining to his or her "person" and therefore maintains a reasonable expectation of privacy in genetic information. The plain text of the Fourth Amendment specifically protects the "right of the people to be secure in their *persons*."[330] In *Kyllo v. United States*,[331] the Court determined that intimate details from within the home were private and reasoned that the Fourth Amendment, at a minimum, protects privacy interests associated with an individual's "house."[332] Similarly, the Fourth Amendment may be construed as inherently protecting privacy that implicates one's body and personhood.[333]

As Sonia Suter has asserted, "Genetic information is central to th[e] development of identity and conceptualization of [the] self."[334] As a result, individuals likely maintain a right to "control the disclosure of personal facts" associated with their unique genetic material.[335] Therefore, even where the "exclusive license" granted to the DTC provider purports to transfer control and use of the Informant's genetic information, the individual nonetheless retains ultimate control of that information because it is his or her private property.

In addition, the notion that the "license" granted to DTC providers does not constitute a transfer of ownership and control is supported by case law concerning the patentability of DNA segments. In *Ass'n for Molecular Pathology v. Myriad Genetics, Inc.*,[336] the Court firmly asserted that "naturally occurring" isolated DNA segments are not patentable and therefore are not subject to ownership by a third party.[337] Applying this holding to genetic information would suggest that third-party DTC providers are not entitled to claim ownership or exclusive use over the Informant's genetic information.

Alternatively, Natalie Ram, a leading legal scholar on the constitutionality of DNA searches, has suggested that genetic information is best understood as being held by an individual as a tenancy by the entirety with all other individuals who share that genetic information.[338] From this perspective, the

329. *See supra* Part I.B.3.a.
330. U.S. CONST. amend. IV (emphasis added).
331. 533 U.S. 27 (2001).
332. *Id.* at 34–38.
333. *See* KRIMSKY & SIMONCELLI, *supra* note 49, at 121.
334. Suter, *supra* note 38, at 333–34.
335. *Id.* at 332–33.
336. 569 U.S. 576 (2013).
337. *Id.* at 580; *see also* Melissa L. Sturges, Comment, *Who Should Hold Property Rights to the Human Genome? An Application of the Common Heritage of Humankind*, 13 AM. U. INT'L L. REV. 219, 232–34, 241–42 (1997).
338. *See generally* Ram, *supra* note 76.

individual disclosing data to a third-party DTC provider cannot vest property rights in the provider because "a key feature of tenancy by the entirety is that typically '[n]either spouse may unilaterally alienate or encumber the property.'"[339] Ram's formulation thus recognizes the shared proprietary interests of the Informant, Target, and Collective in genetic material and each party's associated privacy interests in that material.[340] Pursuant to Ram's perspective, generational consent would likewise have to be granted by the Collective in order for the Informant to convey property interests in his or her genetic material.[341]

Finally, a handful of states have enacted legislation specifying ownership rights over the human genome.[342] These states, which include Alaska, Colorado, Florida, and Georgia, declare that genetic information is the exclusive property of the individual to whom the information belongs.[343] Although state law is by no means conclusive on this matter, it suggests that there is reasonable public support for the understanding that individuals maintain a property interest in their genetic information.

Concepts of property law as applied to genetic information therefore can bolster arguments that the Informant retains a reasonable expectation of privacy in his or her genetic information because the Informant's proprietary interest in that data is not conveyed to the DTC provider. On these grounds, the third-party doctrine should not apply to genetic information because genetic information is protected under the Fourth Amendment as private information associated with protected proprietary interests. In addition, pursuant to Justice Gorsuch's assertions in *Carpenter*, a third-party DTC provider functions as a bailee and may refuse to turn over a consumer's genetic information.[344]

IV. SAFEGUARDING THE RIGHT TO GENETIC PRIVACY

The lack of regulatory or legislative oversight of DTC providers and law enforcement's potential ability to perform warrantless searches of their databases is extremely troublesome in light of individuals' privacy interests in their intimate genetic information. Senator Chuck Schumer called for greater regulation of DTC providers and their capacity to share consumers' genetic information in December 2017.[345] However, no other legislators

339. *Id.* at 912 (alteration in original) (quoting United States v. Craft, 535 U.S. 274, 282 (2002)).

340. *Id.* at 898–903.

341. *See supra* note 277 and accompanying text; *see also* Ram, *supra* note 76, at 913.

342. Ram, *supra* note 76, at 894; *see also Genome Statute and Legislation Database Search*, NAT'L HUM. GENOME RES. INST., https://www.genome.gov/policyethics/legdatabase/pubsearchresult.cfm?content_type_id=1&topic=4&topic_id=1&source_id=1&keyword=&search=Search [https://perma.cc/N3F4-WBMD] (last visited Apr. 10, 2019).

343. SHELDON KRIMSKY & DAVID CAY JOHNSTON, COUNCIL FOR RESPONSIBLE GENETICS, ANCESTRY DNA TESTING AND PRIVACY: A CONSUMER GUIDE 31 (2017), http://www.councilforresponsiblegenetics.org/img/Ancestry-DNA-Testing-and-Privacy-Guide.pdf [https://perma.cc/A8HY-3KMF].

344. *See supra* notes 179–81 and accompanying text.

345. *See* Schulson, *supra* note 275.

have expressed similar sentiments or made efforts to either encourage greater oversight by federal regulators, like the Federal Trade Commission, or expand HIPAA's protections to DTC providers despite extensive media coverage of DTC providers and their privacy policies in the past year.[346] It is thus likely that the burden will ultimately fall to the judiciary to take an active role in protecting privacy interests in genetic information in the context of law enforcement searches of DTC genetic databases.

Genetic testing reveals fundamentally intimate information about an individual that should be protected by the Fourth Amendment—law enforcement officers seeking this information should be required to obtain a warrant supported by probable cause.[347] Part IV.A asserts that judicial intervention to protect the privacy interests of consumers in genetic information would be appropriate in light of current legislative inaction. Part IV.B contends that *Carpenter*'s protections of privacy interests in intimate information disclosed to a third party undoubtedly justifies excluding genetic information from the third-party doctrine under the Fourth Amendment. Part IV.C then describes why *Carpenter*'s approach to the third-party doctrine is preferable to the property-based approach advocated by Justice Kennedy and Justice Gorsuch given the scientific benefits of permitting third-party ownership of genetic information.

A. The Benefits of Judicial Intervention as Opposed to Legislative or Private Solutions

It is emphatically the judiciary's role to analyze the Constitution and protect fundamental privacy interests.[348] As Justice Harlan has stated, "[T]he burden of guarding privacy in a free society should not be on its citizens."[349] Indeed, the presumption that there will be sufficient public demand to stimulate significant legislative action if individuals are dissatisfied with law enforcement's access to private DTC genetic databases is probably unsound.[350] Typically, consumers are not proactive about protecting their privacy interests in information disclosed to third-party providers.[351] For example, the survey conducted to gauge public opinion regarding law enforcement searches of DTC genetic databases solicited participants' opinions on *Carpenter* for the purpose of comparison.[352] The study found "exactly the same pattern of strong support for police access to cell phone records and social media accounts except when the purpose is to identify perpetrators of nonviolent crimes."[353] It is therefore unlikely that consumers

346. *See supra* Part I.B.3.
347. *See supra* Part III.C.2.
348. *See* Marbury v. Madison, 5 U.S. (1 Cranch) 137, 177 (1803); *see also* Olivier Sylvain, *Failing Expectations: Fourth Amendment Doctrine in the Era of Total Surveillance*, 49 WAKE FOREST L. REV. 485, 512 (2014).
349. United States v. White, 401 U.S. 745, 793 (1971) (Harlan, J., dissenting).
350. *See* Sylvain, *supra* note 348, at 491.
351. *See id.* at 491–92.
352. *See* Guerrini et al., *supra* note 243, at 4; *see also supra* Part III.B.2.b.
353. *See* Guerrini et al., *supra* note 243, at 4.

take care to fully educate themselves regarding privacy risks associated with unrestrained searches of their private genetic information by law enforcement or that they take preemptive steps to prohibit such searches.

In the absence of legislative regulation of the disclosure of intimate genetic information, the burden shifts to the DTC providers to regulate such disclosures.[354] Even if we assume that these DTC providers will actually resist such legal requests, it will be difficult for them to do so without a legal determination that the third-party doctrine does not apply.[355] The DTC provider could attempt to narrow a law enforcement subpoena on the grounds of "unreasonable burden," as Google did in California; however, other jurisdictions have not found this legal argument persuasive.[356] If the DTC provider cannot narrow the subpoena, DTC providers would not have grounds to assert Fourth Amendment protection of such information because of the third-party doctrine.[357] Exclusion of genetic information from the third-party doctrine consequently may be necessary in order to allow DTC providers to effectively resist such requests and require a warrant supported by probable cause.

B. Extending Carpenter*'s Protections to Genetic Information Held by Third-Party DTC Providers*

To be clear, in *Carpenter*, the Court asserted that its decision was a "narrow one" that did not "disturb the application of *Smith* [or] *Miller*."[358] However, *Carpenter*'s in-depth consideration of the ways in which individuals casually, and often inadvertently, trade in private and intimate information with third-party providers nonetheless profoundly changes the application of the third-party doctrine analysis.[359] Proof of disclosure to the third-party business has become only the first step in analyzing reasonable expectations of privacy under the third-party doctrine.[360] In *Carpenter*, the Court effectively called for a more in-depth analysis of the premise of assumption of risk and a consideration of more abstract conceptions of privacy that are subject to protection under the Constitution.[361] A searching analysis of this nature of the disclosure of genetic information to DTC providers clearly calls for "genetic exceptionalism" in the context of the third-party doctrine.[362]

Genetic information is inseverable from one's individual identity and reveals deeply personal and sensitive information regarding individuals and

354. *See supra* Part III.B.2.a.
355. *See supra* Part III.B.2.a.
356. *See, e.g.*, United States v. Golden Valley Elec. Ass'n, 689 F.3d 1108, 1115–16 (9th Cir. 2012); Cohen v. City of New York, 255 F.R.D. 110, 121 (S.D.N.Y. 2008).
357. *See supra* note 142 and accompanying text.
358. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).
359. *See* Ohm, *supra* note 148 (manuscript at 3–5).
360. *See supra* Part II.B.2.
361. *See supra* Part II.B.2.
362. *See supra* Parts III.B.2, III.C.2.

their family members.[363] Trading in this confidential information with DTC providers has nonetheless become a relatively casual process in the past three years. Such tests can be easily obtained from drugstores, Amazon, and the providers' websites for a reasonable cost. The decision to disclose this intimate information to a trusted DTC provider is often guided by a strong desire to learn more about one's identity and prepare for potential medical risks through the genetic test.[364] The perspective that disclosing this information to a DTC provider is functionally equivalent to abandoning one's DNA in public therefore seems deeply at odds with the purpose of such disclosure by consumers.[365]

Furthermore, DTC providers, to some extent, mislead consumers as to their capacity to protect consumers' confidential genetic information from access by law enforcement and deanonymization by other parties.[366] These providers indicate that they will actively prevent law enforcement from accessing genetic information while simultaneously reserving their right to do so deep within their terms of use and privacy policies.[367] Consequently, the presumption that consumers assume the risk of law enforcement access within this context may be unwarranted given the purpose of disclosure and probable lack of understanding of the depth of this risk.[368]

If consumers have not assumed the risk of disclosure of their genetic information, the intimate content of such information clearly warrants protection under the Constitution.[369] Genetic information stored in DTC genetic databases reveals far more detailed information than the DNA information stored in CODIS that is used for identification of suspects.[370] There are no current legislative constraints on the scope of genetic information that law enforcement may request from a DTC provider, and thus there is no guarantee they would seek the minimum amount of information needed to identify a suspect.[371]

The medical and familial information revealed by genetic material undoubtedly falls within the bounds of privacy interests traditionally safeguarded under the Constitution.[372] To allow the state to collect and indefinitely retain information concerning medical propensities and familial relationships of individuals by obtaining their genetic information from a DTC provider would be fundamentally at odds with constitutional protections of those realms of privacy from government intrusion.[373] Although the benefits of solving violent cold cases through searches of DTC genetic databases would likely be significant, the countervailing privacy

363. *See supra* Part III.C.2.a.
364. *See supra* Part I.B.2.
365. *See supra* Parts III.B.2.a, III.C.2.a.
366. *See supra* Part III.C.1.
367. *See supra* Part III.C.1.
368. *See supra* Part III.C.1.
369. *See supra* Part III.C.2.a.
370. *See supra* Part III.C.2.a.
371. *See supra* Parts I.B.3, III.C.2.
372. *See supra* Parts II.B.2.a, III.C.2.a.
373. *See supra* Parts II.B.2.a, III.C.2.a.

interests of consumers are also considerable and should be accorded equal weight in the analysis.[374]

Finally, permitting programmatic searches of DTC genetic databases circumvents both the meaningful limits that courts and legislatures have imposed on familial searches of CODIS and the prohibition of suspicionless searches under the Fourth Amendment.[375] The breadth of DTC genetic databases will likely expand to encompass the genetic information of an even more sizeable percentage of the U.S. population as DTC genetic testing continues to grow in popularity.[376] Case law on the scope of CODIS clearly establishes that there is a minimum permissible degree of individualized suspicion of offenders and arrestees that justifies the inclusion of seventeen million DNA profiles in CODIS.[377] No such individualized suspicion inheres in a database of voluntarily disclosed genetic profiles from millions of ordinary citizens; thus, a search of such a database constitutes a suspicionless search.[378] Although such searches may balance out the racial disparities inherent in CODIS, this is a highly indirect method of correcting the racial biases that permeate the criminal justice system, and thereby CODIS.[379] Legislators and law enforcement should instead be encouraged to actively reform CODIS and the criminal justice system at large.

Accordingly, an evaluation of genetic information pursuant to *Carpenter*'s framework overwhelmingly suggests that law enforcement should not have unfettered access to genetic information held by DTC providers as a result of the third-party doctrine. Instead, private genetic information must be protected under the Fourth Amendment, and law enforcement should be required to obtain a warrant supported by probable cause that would narrow and focus a search of a DTC genetic database.

C. Preventing Indivisible Property Interests in Genetic Material

Courts should not, however, evaluate the disclosure of genetic information to third-party DTC providers using the property-based approach articulated in the dissents to *Carpenter*. Granting individuals an indivisible proprietary interest in their genome would have an extreme ripple effect on the field of biomedical research.[380] Biomedical research using genetic material has measurable benefits to the public in developing new treatments for medical conditions.[381] Funding for such research typically is incentivized by the potential to profit from patents on technology derived from such research.[382] A judicial determination that consumers have an indivisible proprietary interest in genetic information disclosed to a DTC provider could

374. *See supra* Parts II.B.2.a, III.C.2.a.
375. *See supra* Parts I.A, III.C.2.b.
376. *See supra* Part I.B.1.
377. *See supra* Part I.A.
378. *See supra* Part III.C.2.b.
379. *See supra* Part III.B.2.b.
380. *See supra* Part III.B.3.
381. *See supra* Part III.B.3.
382. *See supra* Part III.B.3.

inadvertently disrupt this system and, moreover, is not supported by most case law.[383]

In addition, as Sonia Suter has powerfully argued, privacy considerations are a better tool to protect individual's genetic information as opposed to proprietary considerations because privacy law is more attuned to the "dignitary harm and breach of trust" that can result from misuse of genetic information.[384] Indeed, the risk in the disclosure of genetic information to law enforcement is, in large part, the "dignitary harm" caused by government intrusion into medical and familial privacy and not some sort of loss of a presumed proprietary interest in genetic information. It is consequently better to determine whether law enforcement searches of DTC databases are permissible under the Fourth Amendment by reference to the *Carpenter* majority's content-based analysis, which can take into account more abstract privacy interests that can be harmed through government intrusion and surveillance.

CONCLUSION

The benefits that result from using genetic databases to identify suspects in cold cases are concrete and tangible. Through a single search, law enforcement officers might find a violent criminal or sexual predator who has eluded them for decades. However, the intangible harms that result from government surveillance of intimate genetic information can have a significant impact on individuals' sense of security from the government and warrant considerable protections under the Fourth Amendment.

As third-party providers collect more and more information about consumers, perhaps legislatures will become more proactive about regulating such providers. Yet, in the absence of such legislation, there are strong legal grounds to object to warrantless law enforcement searches of private genetic databases on the basis of *Carpenter*. If the Court in *Carpenter* found that reasonable expectations of privacy foreclosed the warrantless disclosure of a comprehensive record of one's movements to the government, it is difficult to rationalize that the same protections should not be afforded to genetic material that undoubtedly reveals a host of intimate and highly personal information pertaining to one's identity, hereditary conditions, and familial relationships. The oversight of government searches afforded by the Fourth Amendment and the warrant requirement can ensure that privacy interests in genetic information will only be compromised if absolutely necessary and that the search will be limited in scope. Such limits on the third-party doctrine are undoubtedly necessary to preserve consumers' personal liberties and prevent invasive surveillance by law enforcement in the twenty-first century.

383. *See supra* Part III.B.3.

384. *See* Sonia M. Suter, *Disentangling Privacy from Property: Toward a Deeper Understanding of Genetic Privacy*, 72 GEO. WASH. L. REV. 737, 749 (2004).