American University Law Review

Volume 68 | Issue 3 Article 5

2019

DNA and Law Enforcement: How the Use of Open Source DNA Databases Violates Privacy Rights

Christine Guest
American University Washington College of Law

DNA and Law Enforcement: How the Use of Open Source DNA Databases Violates Privacy Rights

COMMENTS

DNA AND LAW ENFORCEMENT: HOW THE USE OF OPEN SOURCE DNA DATABASES VIOLATES PRIVACY RIGHTS

CHRISTINE GUEST*

DNA testing, once an expensive and rare technology, has expanded rapidly in the past few decades. Now, individuals can send away a DNA sample for testing at a private company and receive a report with their ancestors' countries of origin and their potential for developing genetically linked diseases within a few weeks. Individuals can even upload these test results to open source websites in order to connect with other individuals who may be related to them. Law enforcement has recognized the value in this technology and begun uploading DNA samples from unknown suspects in order to solve long-cold cases, including the high-profile "Golden State Killer" case. However, open source DNA databases are unlike law enforcement databases. In an open source database, there is no guarantee that an uploaded DNA profile is secure, even if the user is supposedly anonymous. Additionally, the DNA testing technique used to test the DNA sample reveals far more information about the individual, including sensitive information about the suspect's ancestral origin and potential for developing certain genetically-linked diseases.

This Comment argues that when law enforcement uploads a suspect's DNA to an open source DNA database, it violates the suspect's constitutional right to privacy. A suspect retains a privacy interest in some kinds of sensitive information, and by

* Junior Staff Member, *American University Law Review*, Volume 68; J.D. Candidate, May 2020, *American University Washington College of Law*; B.S., Political Science, 2015, *Drexel University*. I am grateful for the hard work of the staff of the *American University Law Review*, Professor Robert Tsai, and Professor Elizabeth Beske, all of whom provided valuable assistance in preparing this piece for publication. I would like to thank my husband, Johnathan Guest, for his support throughout my law school career and my sister and parents for encouraging my love of learning.

uploading the sample to a website accessible to anyone, law enforcement has violated that privacy interest. This Comment further argues that the right to privacy of the suspect's family is also violated by law enforcement use of this technique. Because DNA is shared between genetic relatives, law enforcement is also releasing information that implicates the suspect's genetic relatives any time it uploads a genetic sample to an open source database.

TABLE OF CONTENTS

INTRODUCTION

On April 25, 2018, law enforcement arrested Joseph James DeAngelo, a seventy-two-year-old resident of a Sacramento, California suburb, for a string of rapes and murders committed in the 1970s and 1980s.[1] The killer had eluded law enforcement for decades and was previously known only as the "Golden State Killer," the "Original Night Stalker," and the "East Area Rapist."[2] Shortly after the arrest, details surfaced regarding law enforcement's method for catching the alleged killer. Law enforcement revealed that it had uploaded the unknown suspect's DNA to a DNA database called GEDmatch, an open source website that allows users to upload their genetic profiles from consumer genetic testing sites like Ancestry and 23andMe and make the profiles public to other GEDmatch users.[3] Law enforcement had recovered the suspect's DNA from evidence at several crime scenes, and while the DNA connected the crimes to each other, the DNA never matched any of the profiles in law enforcement's own DNA databases.[4] Officers stated that they had used the suspect's uploaded DNA sample to identify a biological relative and then identified other individuals in the matched user's family tree, ultimately leading the officers to DeAngelo.[5]

The arrest of the Golden State Killer was a highly public instance of law enforcement using genetic data uploaded by private individuals to a public DNA database, rather than using state and federal databases, which are more commonly associated with crime-solving.[6] Private use of genetic testing has expanded rapidly in recent years, with sites like

---

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

2. *Id.*; Laura Miller, *How Did Police Find the Golden State Killer Suspect? Michelle McNamara's Researcher Has a Hunch.*, SLATE (Apr. 25, 2018, 10:03 PM), https://slate.com/news-and-politics/2018/04/paul-haynes-researcher-for-ill-be-gone-in-the-dark-on-how-police-found-the-golden-state-killer-suspect.html.

3. *DNA Used in Hunt for Golden State Killer Previously Led to Wrong Man*, NBC NEWS (Apr. 28, 2018, 3:45 PM) [hereinafter *DNA Previously Led to Wrong Man*], https://www.nbcnews.com/news/us-news/dna-used-hunt-golden-state-killer-previously-led-wrong-man-n869796.

4. *See* Miller, *supra* note 2.

5. *Id.*; Eric Ortiz, *Golden State Killer Suspect's Capture Sparks DNA Site Privacy Fears*, NBC NEWS (Apr. 27, 2018, 7:17 PM), https://www.nbcnews.com/news/us-news/golden-state-killer-suspect-s-capture-sparks-dna-site-privacy-n869661.

6. *See* Matthew Shaer, *The False Promise of DNA Testing*, ATLANTIC (June 2016), https://www.theatlantic.com/magazine/archive/2016/06/a-reasonable-doubt/480747 (discussing the "CSI effect," where jurors expect to see DNA evidence in all trials).

Ancestry and 23andMe boasting millions of users in their databases.[7] Users of these services send in a saliva sample and receive test results with information about their genetics, such as their ancestral countries of origin.[8] Users may also elect to share certain identifying information about themselves with other users whom the testing service identifies as possible biological relatives.[9] Other sites permit users to upload their genetic profiles and make them public to any other user of the site.[10] These public sites are open source, meaning that anyone can access them—including law enforcement.[11]

Many of the articles concerning law enforcement's methodology published in the immediate aftermath of the Golden State Killer arrest wrestle with optimism for the future of this technique to identify suspects in unsolved cases and wariness of the technique's privacy implications.[12] Regardless of the public's trepidation, law enforcement has expanded upon the use of this technique, particularly in cold cases.[13] Technology company Parabon Nanolabs has offered assistance to law enforcement in testing DNA samples for upload to sites like

---

7. *See* Jamie Ducharme, *A DNA Site Helped Authorities Crack the Golden State Killer Case. Here's What You Should Know About Your Genetic Data Privacy*, TIME (Apr. 27, 2018) http://time.com/5257474/golden-state-killer-genetic-privacy-concerns (stating that 23andMe has over five million users); *Company Facts*, ANCESTRY, https://www.ancestry.com/corporate/about-ancestry/company-facts (last visited Feb. 5, 2019) (noting that Ancestry has tested the DNA of over ten million people).

8. *See DNA*, ANCESTRY, https://www.ancestry.com/dna (last visited Feb. 5, 2019) (describing Ancestry's consumer DNA testing services); *see also How 23andMe Works*, 23ANDME, https://customercare.23andme.com/hc/en-us/articles/227968028-How-23andMe-works (last visited Feb. 5, 2019).

9. *See, e.g.*, *Your Privacy*, ANCESTRY, https://www.ancestry.com/cs/legal/privacy statement (last visited Feb. 5, 2019).

10. *See, e.g.*, *GEDmatch.Com Terms of Service and Privacy Policy*, GEDMATCH, https://www.gedmatch.com/tos.htm (last updated May 20, 2018) [hereinafter *GEDmatch Terms of Service*]; OPENSNP, https://opensnp.org (last visited Feb. 5, 2019).

11. *See GEDmatch Terms of Service*, *supra* note 10 (warning users that law enforcement may use the open source database to conduct familial searches to identify a suspect).

12. Ducharme, *supra* note 7 (indicating concern that even if people do not read privacy policies stating that genetic information may be shared, the search for genetic material is analogous to using search engines or social media—both of which have generated serious privacy concerns).

13. *See How a Genealogist Helped Police Crack an Infamous 30-Year-Old Cold Case*, CBS NEWS (July 17, 2018, 7:35 AM), https://www.cbsnews.com/news/april-tinsley-murder-police-crack-cold-case-with-cutting-edge-genealogy. *See generally What is a Cold Case?*, NAT'L INST. OF JUST., https://www.nij.gov/journals/260/pages/what-is-cold-case.aspx (last visited Feb. 5, 2019) (defining cold case as "any case whose probative investigative leads have been exhausted" and noting that relatively short cases may be considered "cold" if there are no fresh leads).

GEDmatch,[14] and many law enforcement bodies have taken advantage of such offers to solve criminal cases.[15]

Any profile created by law enforcement on a public DNA database is also public, at least to a certain degree.[16] The DNA testing procedures used to obtain the correct format for uploading to a public DNA database are also far more "intrusive" than DNA testing traditionally used by law enforcement.[17] While the DNA tests used by law enforcement for inclusion in government databases reveal nothing about the individual's ancestry or medical history, the testing performed by commercial DNA databases is specifically designed to provide personal information, such as the individual's genetic predisposition for certain diseases.[18] By uploading a suspect's DNA on a site like GEDmatch, law enforcement is revealing a great deal of highly sensitive data about the suspect to an unknown number of third parties. Additionally, because DNA is shared between relatives, uploading a suspect's DNA profile to a public website may also share data about the suspect's biological relatives.[19]

This Comment argues that the sensitivity of the information revealed by a suspect's genetic profile is so great that the suspect and the suspect's family maintain a privacy interest in that genetic information. As such, law enforcement violates both the suspect's right to privacy and the suspect's relatives' rights to privacy when law enforcement uploads the suspect's DNA profile to an open source DNA database. While this Comment cites to several Fourth Amendment decisions, this Comment bases its argument solely on the grounds of the right to privacy. Any citation to Fourth Amendment jurisprudence is used only to highlight the privacy interests protected by the courts in those cases. Additionally, while the anonymization of an individual's data may seem

---

14. *See Parabon® Announces Snapshot® Genetic Genealogy Service for Law Enforcement,* PARABON NANOLABS (May 8, 2018), https://parabon-nanolabs.com/nanolabs/news-events/2018/05/parabon-snapshot-genetic-genealogy-dna-analysis-service.html.

15. *See* Kate Snow and John Schuppe, *'This is Just the Beginning': Using DNA and Genealogy to Crack Years-Old Cold Cases*, NBC NEWS (July 18, 2018, 4:30 AM), https://www.nbcnews.com/news/us-news/just-beginning-using-dna-genealogy-crack-years-old-cold-cases-n892126.

16. *See GEDmatch Terms of Service* , *supra* note 10 (warning users of the potential privacy implications of uploading their genetic information to the website and clarifying that although the underlying raw DNA is modified from its original form, the transformed data is not kept in an encrypted format).

17. *See infra* Section II.A.1.

18. *See infra* Section I.A.2.

19. *See infra* Section I.A.1.

to negate privacy concerns, there is no guarantee that this data will remain anonymous, particularly after a high-profile suspect is identified in the media.[20] Some may also argue that a suspect does not maintain a privacy right in information revealed by crime scene DNA, but courts have recognized a right to confidentiality for certain kinds of sensitive information, even for individuals with reduced privacy rights.[21]

Part I of this Comment begins by providing some scientific background on DNA and then goes on to describe DNA testing techniques, focusing on the testing techniques used by law enforcement and private DNA testing services.[22] This section further elaborates on the rise of direct-to-consumer DNA testing and the leaps in technology that now allow DNA tests to reveal far more information about an individual than previous DNA tests.[23] Finally, Part I discusses the development of the constitutional right to privacy and the applicability of this right in analogous contexts.[24]

Next, Part II of this Comment analyzes the law enforcement practice of uploading a suspect's DNA to a publicly available DNA database in the context of the applicable law discussed in Part I. Section II.A discusses the privacy rights of a suspect and argues that some of the information contained within an individual's DNA implicates sensitive information about the individual's health and genetic background. Therefore, law enforcement violates a suspect's right to privacy by uploading the DNA profile to a website where the public can potentially access the information. Section II.B discusses the privacy rights of a suspect's family members. This section argues that the information contained in a suspect's DNA can also reveal sensitive information about a suspect's family members. Because uploading the DNA profile implicates the privacy rights of innocent third parties, law enforcement is therefore obligated to keep this information confidential.

I. BACKGROUND

A. The Basics of DNA and DNA Testing

A basic understanding of the science of DNA is essential to understand how law enforcement uses DNA to identify suspects in cold

20. *See infra* Section I.C.2.
21. *See infra* Section I.D.2.
22. *See infra* Sections I.A, I.B.
23. *See infra* Section I.C.
24. *See infra* Section I.D.

cases. This section will address several important points, including what DNA is, how related individuals share DNA, and how scientists test DNA.

1. DNA and shared biological characteristics

DNA stands for "deoxyribonucleic acid," and is found in most cells of the body of a living thing.[25] DNA is essentially a "blueprint" that tells the body how to make different types of proteins.[26] To form this "blueprint," DNA has four "bases" called adenine (A), cytosine (C), guanine (G), and thymine (T).[27] These bases match up with one another to form the unique twisted ladder shape of a DNA molecule, known as a "double helix."[28] The bases always match with a particular counterpart (A always matches with T and C always matches with G) to form a "base pair."[29] DNA coils itself into compact structures called chromosomes, which are stored in the nucleus of the cell.[30] Most cells in the human body contain forty-six chromosomes, each made of tightly compacted DNA.[31] Collectively, all of the information contained within an individual's DNA is called the individual's "genome."[32] The genome of one individual human contains approximately 3.2 billion base pairs.[33] DNA is also able to make copies of itself, which allows cells to divide and form new cells with the same exact DNA.[34]

DNA is a hereditary material, meaning that it is passed down from parents to their biological children.[35] Hereditary information concerns both "phenotype," the physical manifestation of a genetic trait, and "genotype," the underlying genetic code that informs the creation of the trait.[36] A biological child, however, can inherit traits from a parent that

---

25. *What is DNA?*, NIH, U.S. NAT'L LIBR. OF MED.: GENETICS HOME REFERENCE (July 17, 2018) [hereinafter *What is DNA?*], https://ghr.nlm.nih.gov/primer/basics/dna.

26. A. JAMIE CUTICCHIA, GENETICS: A HANDBOOK FOR LAWYERS 16 (2d ed. 2018).

27. *What is DNA?*, *supra* note 25.

28. *Id.*

29. *Id.*

30. CUTICCHIA, *supra* note 26, at 5.

31. *Id.* at 5, 9. Additionally, some individuals can have more or less than forty-six chromosomes, a condition known as aneuploidy, which is often connected to other genetic diseases. *See id.* at 11.

32. *Id.* at 8.

33. *Id.*

34. *What is DNA?*, *supra* note 25.

35. *See, e.g.*, Anthony J.F. Griffiths et al., *DNA: The Genetic Material*, *in* AN INTRODUCTION TO GENETIC ANALYSIS 260 (2000); Timothy Newman, *What is DNA and How Does it Work?*, MEDICAL NEWS TODAY (Jan. 11, 2018), https://www.medicalnewstoday.com/articles/319818.php.

36. CUTICCHIA, *supra* note 26, at 19–20.

the parent does not outwardly demonstrate.[37] This is because the child's parents may have passed down DNA with recessive genes, which are only expressed when the child does not inherit a dominant gene from a parent.[38]

Because a child inherits DNA from both parents, who in turn inherited their DNA from their parents, and so on, each person shares DNA not only with his parents, but also with other biologically related members of his family. Closely related individuals usually share a significant amount of DNA with one another.[39] However, with the exception of the parent-child relationship, the exact amount of shared DNA between related individuals varies depending on how close the genetic relationship is between the two individuals.[40] The closer the genetic relationship between the two individuals, the more likely they are to share a significant amount of DNA.[41] However, at some point when two individuals are very distantly related, they may not share any DNA at all.[42]

2. Identifying individuals using DNA

DNA is unique to each individual.[43] Therefore, by testing DNA, scientists can compare a DNA sample from an unknown individual to DNA from known individuals to try and find a match.[44] To match one sample of DNA to another, scientists can create a "DNA fingerprint," which isolates certain elements of the DNA in a sample to create a

37. *Id.* at 20–21.

38. *Id.*

39. CeCe Moore & Henry Louis Gates Jr., *How Much DNA Do Distant Cousins Actually Share?*, THE ROOT (Nov. 14, 2014, 3:00 AM), https://www.theroot.com/how-much-dna-do-distant-cousins-actually-share-1790877726.

40. *Id.*

41. *Id.*

42. With modern testing techniques used by consumer DNA testing services, true third cousins are read as unrelated to one another approximately ten percent of the time because they may not have received any of the same DNA from their shared second-great-grandparents. *Id.*

43. *See* CUTICCHIA, *supra* note 26, at 29 (discussing genetic variation in humans). While some often believe that identical twins, because they come from the same egg which splits *in utero* to create two individuals, have identical DNA, recent studies have demonstrated that even identical twins have some small genetic variations. *See* Peter Miller, *A Thing or Two About Twins*, NAT'L GEOGRAPHIC MAG. (Jan. 2012), https://www.nationalgeographic.com/magazine/2012/01/identical-twins-science-dna-portraits (stating that identical twins share *almost* identical DNA).

44. *See* CUTICCHIA, *supra* note 26, at 81–85 (describing early and more modern methods for comparing samples of DNA in forensic analysis).

unique profile that can then be matched to other DNA samples.[45] To create a DNA fingerprint, the scientist must first have a sample to work from.[46] This sample can be from any DNA-containing material, including blood, saliva, or skin.[47]

Once the scientist has a sample, he may choose from a variety of testing methods to create a DNA fingerprint. While older methods of DNA testing required a significant amount of DNA, the same is not true of more modern techniques. With modern DNA testing, even small amounts of DNA and degraded DNA can be tested using the polymerase chain reaction (PCR) technique.[48] PCR replicates certain sequences within the DNA molecule to create enough DNA material to test.[49]

After a scientist has enough genetic material to test, there are a couple different modern testing methods that he can use to create the DNA fingerprint. One method is to test for "short tandem repeats" (STRs) within the DNA sample.[50] These STRs can repeat dozens or hundreds of times throughout the individual's genome, and the number of times STRs repeat varies from person-to-person.[51] Testing a variety of STRs can provide the scientist with enough unique information to reliably identify an individual.[52] STRs are not genes, so they do not reveal much information about the individual; however, by testing for enough STRs, a scientist can create a profile that can be compared to other DNA samples for identity purposes.[53]

Another method of testing DNA is to test for single-nucleotide polymorphisms (SNPs). SNPs do not vary as much as STRs, but by testing for enough SNPs, the scientist can create a reliable DNA fingerprint for an individual.[54] SNPs do, however, indicate what a

---

45. Editors of the Encyclopaedia Britannica, *DNA Fingerprinting*, ENCYCLOPAEDIA BRITANNICA https://www.britannica.com/science/DNA-fingerprinting (last visited Feb. 5, 2019) [hereinafter *DNA Fingerprinting*].

46. *Id.*

47. *See* CUTICCHIA, *supra* note 26, at 50–53 (describing methods of collecting DNA, including blood draws, saliva collection, and sampling shed skin cells).

48. *Id.* at 50–53, 88–90 (describing how PRC techniques operate); *DNA Fingerprinting*, *supra* note 45.

49. *DNA Fingerprinting*, *supra* note 45.

50. *Id.*

51. CUTICCHIA, *supra* note 26, at 85; 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.

52. *See* Zhang, *supra* note 51.

53. *Id.*

54. *Id.* (stating that with enough SNPs one can "trace the geographic origins of ancestors and find distant relatives").

person's ancestry may be, and can provide insight into the individual's probable eye color, race, and geographic ancestry.[55] SNPs can also provide insight into an individual's medical history by showing the individual's susceptibility to certain genetically-linked diseases.[56]

Finally, a scientist may choose to "sequence" the DNA that he is testing.[57] Sequencing is more comprehensive than SNP or STR testing and involves determining the exact sequence of all or a portion of an individual's genome.[58] However, this technology can be expensive and is therefore often unavailable on a large scale.[59] The price of this technology continues to fall, however, and the National Institute of Health's National Human Genome Research Institute aims to one day bring the cost of this testing technique to under $1,000.[60]

B. Law Enforcement DNA Collection and Retention

DNA testing was introduced relatively early in legal disputes to solve crimes and determine paternity.[61] However, the large amount of DNA needed for early techniques limited the use of DNA testing in most cases.[62] Today, law enforcement has extensive procedures and resources for using DNA to solve crimes.[63] The Federal Bureau of Investigation (FBI) maintains a national database known as the Combined DNA Index System (CODIS), which also includes a network of state databases and federal databases maintained by other federal entities, known as the

---

55. *Id.*

56. Tina Hesman Saey, *What Consumer DNA Data Can and Can't Tell You About Your Risk for Certain Diseases*, SCI. NEWS (June 3, 2018, 6:00 AM), https://www.sciencenews.org/article/health-dna-genetic-testing-disease (discussing how genetic testing services can now test for risks related to certain genetic diseases).

57. *See* Anthony J.F. Griffiths, *DNA Sequencing*, ENCYCLOPAEDIA BRITANNICA, https://www.britannica.com/science/DNA-sequencing (last visited Feb. 5, 2019) (explaining DNA sequencing and the development of sequencing technology).

58. *What Is the Difference Between Genotyping and Sequencing?*, 23ANDME, https://customercare.23andme.com/hc/en-us/articles/202904600-What-is-the-difference-between-genotyping-and-sequencing (last visited Feb. 5, 2019).

59. *Id.*

60. *DNA Sequencing*, NIH: NAT'L HUM. GENOME RES. INST., https://www.genome.gov/10001177/dna-sequencing-fact-sheet (last visited Feb. 5, 2019).

61. *DNA Fingerprinting*, *supra* note 45.

62. *Id.*

63. *See Advancing Justice Through DNA Technology: Using DNA to Solve Crimes*, DEP'T JUST. ARCHIVES (last updated Mar. 7, 2017), https://www.justice.gov/archives/ag/advancing-justice-through-dna-technology-using-dna-solve-crimes.

National DNA Index System (NDIS).[64] States also frequently have their own internal databases.[65] Whose DNA goes into the database and how that DNA is retained, used, and tested has been the subject of much litigation.[66] This section discusses how law enforcement tests and stores data, who law enforcement may take DNA from, and how law enforcement uses familial DNA testing within its own databases.

1. Law enforcement DNA databases

With the expansion of DNA technology, law enforcement has now created DNA databases for internal use to solve crimes and locate criminals. On the federal level, there is CODIS.[67] CODIS is operated by the FBI, along with NDIS, which has 190 participating local laboratories around the country.[68] CODIS stores the DNA information of convicted offenders, some arrestees, and DNA samples from crime scenes.[69] CODIS is a federal database, but information from state DNA laboratories is also uploaded to CODIS through the NDIS partnership with local laboratories.[70] Initially, CODIS tested DNA at thirteen particular locations, known as loci, but the FBI added seven more loci in January 2017 to ensure the accuracy of DNA matches as the number of profiles uploaded to CODIS increased.[71] The loci tested for the CODIS database are in non-coding regions of an individual's DNA, meaning that they only establish a code that can be used to identify the individual and do not implicate any additional information about the

64. *Frequently Asked Questions on CODIS and NDIS*, FED. BUREAU INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet [hereinafter *CODIS and NDIS FAQs*] (last visited Feb. 5, 2019).

65. *See* Jason Kreag, *Going Local: The Fragmentation of Genetic Surveillance*, 95 B.U. L. REV. 1491, 1500–01 (2015) (discussing the expansion of state and local DNA databases and the privacy implications of this trend).

66. *See, e.g.*, United States v. Davis, 690 F.3d 226, 251 (4th Cir. 2012) (examining the constitutionality of police retention of a DNA sample collected from an individual when he was previously a crime victim and the subsequent creation of a DNA profile to investigate him as a murder suspect); People v. Buza, 413 P.3d 1132, 1135 (Cal. 2018) (upholding a California law that requires police to collect DNA samples from those arrested for or convicted of felony offenses).

67. CUTICCHIA, *supra* note 26, at 86.

68. *Combined DNA Index System (CODIS)*, FED. BUREAU INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis (last visited Feb. 5, 2019). The locations tested in a DNA test are commonly known as "loci." *Id.*

69. CUTICCHIA, *supra* note 26, at 86.

70. *Id.*

71. *Id.* at 86–87.

individual's appearance, ancestral origin, or medical information.[72] State and local law enforcement have their own databases as well.[73] While state and local DNA databases were usually created to retain the DNA data of sex offenders, these databases have expanded to include other DNA profiles.[74] State databases also may be far broader and more inclusive of other DNA samples outside of what the state uploads to the federal system, NDIS.[75]

2. Collection of DNA for inclusion in law enforcement databases

To maintain its databases, law enforcement must collect DNA from individuals. The FBI is authorized to create a DNA index consisting of DNA from "persons convicted of crimes," "persons who have been charged in an indictment or information with a crime," and "other persons whose DNA samples are collected under applicable legal authorities, provided that DNA samples that are voluntarily submitted solely for elimination purposes shall not be included in the National DNA Index System."[76] The FBI is also authorized to include in the DNA index samples from crime scenes, unidentified human remains, and samples provided voluntarily by the relatives of missing persons.[77] The law also provides that to be included in CODIS, the DNA analyses must come from laboratories or state, local, or federal agencies that meet certain guidelines and, in the case of external laboratories, undergo external audits.[78]

A more controversial measure has been the inclusion of the DNA of individuals arrested for certain crimes in law enforcement DNA databases. In *Maryland v. King*,[79] the Supreme Court of the United

72. *Id.* at 87–88.

73. *See* Kreag, *supra* note 65, at 1492. For an interesting discussion of the regulatory problems with state and local DNA databases, see Stephen Mercer & Jessica Gabel, *Shadow Dwellers: The Underregulated World of State and Local DNA Databases*, 69 N.Y.U. ANN. SURV. AM. L. 639, 691–94 (2014), noting that state DNA databases are largely unregulated in some states, and that DNA of victims is sometimes retained in the database despite the fact that the victim did not commit a crime.

74. *See* Mark A. Rothstein & Meghan K. Talbott, *The Expanding Use of DNA in Law Enforcement: What Role for Privacy?*, 34 J.L. MED. & ETHICS 153, 153–54 (2006) (explaining the expansion of local DNA databases).

75. *See* Mercer & Gabel, *supra* note 73, at 654–55 (describing the variation in state practices for what to include in the state's own database, and how what the state includes in its own database may differ from what the state uploads to NDIS).

76. 34 U.S.C. § 12592(a)(1) (Supp. V 2017) (formerly codified at 42 U.S.C. § 14132).

77. § 12592(a)(2)–(4).

78. § 12592(b).

79. 569 U.S. 435 (2013).

States held that a Maryland law permitting police officers to take DNA samples from individuals arrested for, but not convicted of, serious crimes was permissible under the Fourth Amendment.[80] The Maryland law permitted the collection of DNA from individuals arrested for committing a burglary or crime of violence, or attempting to commit a burglary or crime of violence.[81] Since the *King* decision, the federal government has also authorized the collection of DNA from individuals who have been "arrested, facing charges, or convicted" of a crime and individuals who are on "probation, parole, or supervised release."[82]

3. Familial DNA testing in law enforcement DNA databases

The federal government does not explicitly authorize familial DNA testing within its NDIS databases.[83] However, the FBI may perform a "moderate stringency search" of the NDIS system, which can be used to search the DNA database for a match to a sample that contains DNA from multiple individuals or is partially degraded.[84] Moderate stringency searches can also allow scientists to account for variations across different laboratories.[85] Law enforcement may use these moderate stringency tests to capture DNA profiles in the database that contain the same DNA as the sample but that might not show up on a higher stringency test.[86] For example, a moderate stringency search may help law enforcement by matching a suspect's DNA to partially

---

80. *Id.* at 465. In *King*, the Court found that,

> In light of the context of a valid arrest supported by probable cause respondent's expectations of privacy were not offended by the minor intrusion of a brief swab of his cheeks. By contrast, that same context of arrest gives rise to significant state interests in identifying respondent not only so that the proper name can be attached to his charges but also so that the criminal justice system can make informed decisions concerning pretrial custody. Upon these considerations the Court concludes that DNA identification of arrestees is a reasonable search that can be considered part of a routine booking procedure.

Id.

81. *Id.* at 443.

82. 34 U.S.C. § 40702(a) (Supp. V 2017) (formerly codified at 42 U.S.C. § 14135a); *see also* Mercer & Gabel, *supra* note 73, at 652–53 (discussing how both federal and state governments have expanded DNA collection procedures).

83. *CODIS and NDIS FAQs*, *supra* note 64.

84. *Id.*

85. *Id.*

86. *See id.* (defining a high stringency test as one "that requires all alleles to match" between the sample and database profile, while defining a moderate stringency test as one "requires all alleles to match, but [the sample and database profile] can contain a different number of alleles").

degraded DNA the same suspect left at a previous crime scene.[87] There is also a possibility that these moderate stringency tests may return a "partial match" result between two single source samples—two samples that are each known to include only one individual's DNA. Such a result can indicate that the contributors of the two samples may be biologically related to one another, although the FBI notes that the likelihood of a true familial relationship based on a moderate stringency test is low.[88] The FBI may choose to disclose the partial match, and thus a possible familial relationship, to the law enforcement agency conducting the search.[89] However, the FBI considers the reporting of these partial matches not to be the same as familial DNA testing, as the test was not an "intentional or deliberate search" with the purpose of finding related individuals.[90]

In some states, law enforcement uses familial DNA testing within its own databases.[91] Twelve states have used familial DNA testing in their own DNA databases to track down suspects: Arizona, California, Colorado, Florida, Minnesota, New York, Ohio, Texas, Utah, Virginia, Wisconsin, and Wyoming.[92] Very few of these laws have been challenged so far, and courts have generally not answered the question about the implications of familial DNA testing on an individual's relatives.[93] Two jurisdictions, the District of Columbia and Maryland,

87. *Id.*

88. *Id.*

89. *Id.*; *see also* FBI LAB., NAT'L DNA INDEX SYSTEM (NDIS) OPERATIONAL PROCEDURE MANUAL 82–84 (2016), https://www.fbi.gov/file-repository/ndis-operational-procedures-manual.pdf (detailing the NDIS "plan" for releasing the results of a partial match).

90. *CODIS and NDIS FAQs*, *supra* note 64.

91. James Rainey, *Familial DNA Puts Elusive Killers Behind Bars. But Only 12 States Use It.*, NBC NEWS (Apr. 28, 2018, 6:00 AM) https://www.nbcnews.com/news/us-news/familial-dna-puts-elusive-killers-behind-bars-only-12-states-n869711.

92. *Id.*; *see also* Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291, 302–03 (2010) (stating that while some states have formally codified the practice of familial searching in law, other jurisdictions sometimes perform familial searches without statutory authorization).

93. *See* United States v. Mitchell, 652 F.3d 387, 412–13 (3d Cir. 2011) (distinguishing DNA samples, which the court said do contain genetic information about an individual's family, from DNA profiles entered into CODIS, which the court said reveal only the individual's identity, and not addressing the question of privacy in these samples); State v. Athan, 158 P.3d 27, 34 (Wash. 2007) (en banc) (noting that while it may be true that DNA contains information about an individual's family and may constitute a privacy interest, the use of DNA in the case presented a narrower question and therefore the court made no decision regarding privacy interests in DNA). *But see Mitchell*, 652 F.3d at 423–24 (Rendell, J., dissenting) (stating that the

explicitly forbid the use of familial DNA testing in state databases.[94] In academic circles, many argue that familial DNA testing violates Fourth Amendment protections and invades the privacy rights of individuals.[95]

C. The Rise of Consumer Genetic Testing and Public DNA Databases

In recent years, DNA testing has become cheaper and expanded into other markets. Several private DNA testing companies have established a market for direct-to-consumer genetic tests, which provide users with information about their ancestry, potential for developing a genetically-linked disease, and carrier status for certain diseases that the user may pass on to his children.[96] This section explores the rapid expansion of these private genetic testing services, the establishment of public DNA databases, and how law enforcement has increasingly used this technology to solve cold cases.

1. Direct-to-consumer genetic testing services

Direct-to-consumer genetic testing services first appeared in the early 2000s but have rapidly become more accessible because of price reductions.[97] Direct-to-consumer DNA tests have risen drastically in popularity in recent years, and they are expected to continue to grow.[98]

---

majority ignores the vast amount of sensitive genetic information in an individual's DNA sample, which is usually retained by the government).

94. D.C. CODE § 22-4151(b) (2018); MD. CODE ANN., PUB. SAFETY § 2-506(d) (West 2018).

95. *See* Jessica D. Gabel, *Probable Cause from Probable Bonds: A Genetic Tattle Tale Based on Familial DNA*, 21 HASTINGS WOMEN'S L.J. 3, 4–5 (2010) (cautioning the use of familial DNA testing and identifying potential problems); Trevor Woodage, Note, *Relative Futility: Limits to Genetic Privacy Protection Because of the Inability to Prevent Disclosure of Genetic Information by Relatives*, 95 MINN. L. REV. 682, 708–09 (2010) (identifying ways to prevent abuse of familial DNA testing). *But see* David H. Kaye, *The Genealogy Detectives: A Constitutional Analysis of "Familial Searching,"* 50 AM. CRIM. L. REV. 109, 113 (2013) (arguing that properly implemented familial DNA searching is a valuable tool for law enforcement).

96. *See, e.g.*, *Our Services: Health + Ancestry*, 23ANDME, https://www.23andme.com/dna-health-ancestry (last visited Feb. 5, 2019) (explaining the wide range of ancestry and medical tests 23andMe may perform on an individual's DNA sample).

97. 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 (discussing the price war between consumer genetic testing companies); *see also Our Story*, ANCESTRY, https://www.ancestry.com/corporate/about-ancestry/our-story (last visited Feb. 5, 2019); *About Us*, 23ANDME, https://mediacenter.23andme.com/company/about-us (last visited Feb. 5, 2019).

98. Mark Williams, *The Lucrative Rise of DNA Testing: 'We Created the Market for What We Do,'* GUARDIAN (May 25, 2017, 2:00 AM) https://www.theguardian.com/small-

Ancestry, the largest consumer DNA database, now boasts that it has tested approximately 10 million people's DNA.[99] The consumer DNA testing industry has also moved beyond testing for ancestry and now offers other services, such as DNA-specific skincare and fitness routines.[100] Many companies can now offer their genetic testing services for under sixty dollars.[101] The industry took off in the summer of 2016, rapidly expanding from about 2.5 million people tested across the industry to over 12 million people in 2018.[102]

Of the largest companies in the direct-to-consumer DNA testing market, most perform "autosomal" DNA testing to test consumers' DNA samples.[103] Autosomal DNA is the DNA not involved in sex determination.[104] Generally, most companies perform SNP testing as outlined above, testing particular single-nucleotide polymorphisms that indicate a person's ancestral origin.[105] Direct-to-consumer tests include a large number of SNPs in their testing process.[106] For instance, Ancestry purports to test the person's "entire genome at over 700,000 locations."[107] To determine an individual's ancestral origins, these tests compare the individual's DNA sample with other DNA samples to estimate an individual's ancestral background.[108] The advantage to using SNP testing is that it captures the individual's entire genetic background, instead of only certain family genetic lines.[109] This more comprehensive type of testing also allows the industry to offer many more types of DNA analyses, including everything from diet

---

business-network/2017/may/25/dna-testing-we-created-the-market-for-what-we-do-living-dna-dnafit-geneu (noting that the consumer genetic testing industry was worth $70 million in 2015 but is expected to be worth $340 million by 2022).

99. *Company Facts*, ANCESTRY, https://www.ancestry.com/corporate/about-ancestry/company-facts (last visited Feb. 5, 2019).

100. Williams, *supra* note 98.

101. Regalado, *supra* note 97.

102. *Id.*

103. *The Pros and Cons of the Main Autosomal DNA Testing Companies*, DNA GEEK (Nov. 13, 2016), http://thednageek.com/the-pros-and-cons-of-the-main-autosomal-dna-testing-companies.

104. CUTICCHIA, *supra* note 26, at 223.

105. Zhang, *supra* note 51.

106. *What is Genetic Ancestry Testing?*, NIH, U.S. NAT'L LIBR. MED.: GENETICS HOME REFERENCE, https://ghr.nlm.nih.gov/primer/dtcgenetictesting/ancestrytesting (last visited Feb. 5, 2019).

107. *AncestryDNA—Frequently Asked Questions*, ANCESTRY, https://www.ancestry.com/dna/en/legal/us/faq#about-3 (last visited Feb. 5, 2019).

108. *What is Genetic Ancestry Testing?*, *supra* note 106.

109. *Id.*

recommendations to advice regarding genetic health risks.[110] While this Comment addresses privacy rights in the context of open source DNA databases, privately maintained DNA databases have also grappled with privacy rights concerns.[111]

2. Open source DNA databases

Some DNA databases provide open source access to DNA profiles, including the now-famous GEDmatch used in the Golden State Killer investigation.[112] GEDmatch allows users to upload their DNA data generated by an earlier DNA test from a consumer genetic testing service like Ancestry or 23andMe.[113] When GEDmatch users upload their genetic profile to the site, they have the option to designate the genetic profile as "private," "public," or "research."[114] Private DNA "is "available for comparison to any Raw Data in the GEDmatch database using the various tools provided for that purpose."[115] Research DNA may be used for a "one-to-one comparison to other Public or Research DNA."[116]

GEDmatch notes that it does not guarantee the "confidentiality of any communication, material, or personal information provided to GEDmatch via the Site or email."[117] The site also provides the following information about what happens to data once it is uploaded to the site:

> The original Raw DNA and GEDCOM data you provide to GEDmatch is not kept in its original form. It is converted to a form that makes it more efficient for the software to perform searches and comparisons. The Genealogical Data is loaded into a relational database that might still be recognizable as text. The Raw DNA is converted to a compressed binary format in a process we call "tokenization." Although the Raw DNA is not encrypted in the usual sense of the word, it would be very difficult for a human to read it.

---

110. *See* Regalado, *supra* note 97 (noting that there is little oversight of a growing sector which offers to "reanalyze" genetic data and provide products or services based on an individual's genetic makeup).

111. Maggie Fox, *What You're Giving Away with Those Home DNA Tests*, NBC NEWS (Nov. 30, 2017), https://www.nbcnews.com/health/health-news/what-you-re-giving-away-those-home-dna-tests-n824776.

112. Vera Eidelman, *The Creepy, Dark Side of DNA Databases*, WASH. POST (May 8, 2018), https://www.washingtonpost.com/opinions/the-creepy-dark-side-of-dna-databases/2018/05/08/279e9c2c-5230-11e8-abd8-265bd07a9859.

113. Julian Hattem, *Investigators Say DNA Database Can Be a Goldmine for Old Cases*, AP (June 16, 2018) https://www.apnews.com/96ee418316c343649df5d10d2a44c600.

114. *GEDmatch Terms of Service*, *supra* note 10.

115. *Id.*

116. *Id.*

117. *Id.*

> Original uploaded files are deleted from the Site servers soon after they are processed and archived.[118]

GEDmatch also notes that it cannot guarantee users will not access the site for purposes other than genealogical research.[119] GEDmatch states that users of the site may discover another user's identity (even if that user has attempted to obscure the information), genetic relationships between individuals, or medical information.[120] Additionally, the site's user agreement now states that law enforcement may upload DNA to "identify a perpetrator of a violent crime against another individual" or "identify remains of a deceased individual."[121] There is no indication as to how GEDmatch polices or enforces this rule.

3. Law enforcement use of private and public databases

In the Golden State Killer investigation, law enforcement found a particularly well-preserved sample of DNA from one of the crime scenes believed to be connected to the serial killer.[122] Law enforcement uploaded the DNA data of the suspect's sample to GEDmatch and obtained a partial match to an individual that law enforcement believed to be a relative of the suspect.[123] GEDmatch was unaware of this use of its website, and affiliates of the company state that law enforcement use was not part of the concept of the website itself.[124]

Once a law enforcement agency has a partial match to a suspect's profile on a public DNA database, they can use this information to identify likely suspects. Law enforcement can construct the family tree of the matched individual through public records to identify related individuals who fit the profile of the suspect.[125] Once law enforcement has narrowed down the search of the family tree to a particular

---

118. *Id.*
119. *Id.*
120. *Id.*
121. *Id.* (defining "violent crime" as "homicide or sexual assault").
122. Gina Kolata & Heather Murphy, *The Golden State Killer is Tracked Through a Thicket of DNA, and Experts Shudder*, N.Y. TIMES (Apr. 27, 2018), https://www.nytimes.com/2018/04/27/health/dna-privacy-golden-state-killer-genealogy.html.
123. *Id.*
124. *See id.* (explaining that, at the time they uploaded their sample, law enforcement had to certify "that the DNA was their own or belonged to someone for whom they were legal guardians," or that they had received permission to upload the DNA).
125. Heather Murphy, *Technique Used to Find Golden State Killer Leads to a Suspect in 1987 Murders*, N.Y. TIMES (May 18, 2018), https://www.nytimes.com/2018/05/18/science/ancestry-site-arrest-washington.html.

individual, law enforcement may choose to get a warrant for a genetic sample from the suspect.[126] However, under the law established in *California v. Greenwood*,[127] law enforcement may also obtain the suspect's DNA without a warrant.[128] In the Golden State Killer investigation, law enforcement used DNA found on items that DeAngelo had discarded and on public surfaces he had recently touched to determine that he was a match to original crime scene DNA.[129]

Since the success in the Golden State Killer case, law enforcement agencies in other jurisdictions have used GEDmatch in other cases to turn up familial matches to unknown DNA samples left by suspects at crime scenes.[130] GEDmatch's website now warns users that law

---

126. *See DNA Previously Led to Wrong Man*, *supra* note 3 (stating that law enforcement did obtain a warrant in the Golden State Killer investigation to obtain the DNA of another man, who was ruled out as a suspect after DNA testing).

127 486 U.S. 35 (1988).

128. *See DNA From Tissue in Trash Led to Arrest in Golden State Killer Case, Records Show*, CBS NEWS (June 1, 2018) [hereinafter *Tissue Led to Arrest*], https://www.cbsnews.com/news/dna-from-tissue-in-trash-led-to-arrest-in-golden-state-killer-case-records-show (reporting how police tracked DeAngelo by first obtaining a DNA sample from a door handle, and then obtaining another sample from a tissue in DeAngelo's trash); *see also* Aaron Keller, *How 'Discarded DNA' Helped Cops Legally Catch the Suspected Golden State Killer*, LAW & CRIME (Apr. 25, 2018, 5:01 PM), https://lawandcrime.com/high-profile/how-discarded-dna-helped-cops-legally-catch-the-suspected-golden-state-killer (discussing how police did not need to obtain warrants for the DNA samples collected from DeAngelo prior to his arrest because DNA that has been "discarded" by the individual does not receive the same Fourth Amendment protections as DNA taken directly from an individual). Warrantless searches of an individual's discarded trash were held to be constitutional in *California v. Greenwood*, 486 U.S. 35, 37 (1988), but the Supreme Court has declined to rule on the constitutionality of testing "discarded" DNA. *See* Raynor v. State, 99 A.3d 753 (Md. 2014), *cert denied*, 135 S. Ct. 1509 (2015). Multiple state courts have upheld this practice, while federal courts have generally taken a more cautious approach. *See, e.g.*, Schmidt v. Stassi, 250 F. Supp. 3d 99, 107 (E.D. La. 2017) (holding that the swabbing of a Hummer door constituted a Fourth Amendment search, but declining to rule whether DNA analysis of the swab was a Fourth Amendment search); State v. Williford, 767 S.E.2d 139, 144–45 (N.C. Ct. App. 2015) (finding that collection and analysis of a discarded cigarette butt did not implicate the defendant's constitutional rights); State v. Athan, 158 P.3d 27, 37 (Wash. 2007) (en banc) (concluding that police did not violate the Fourth Amendment when they analyzed DNA collected from a sealed letter addressed to their own detectives).

129. *Tissue Led to Arrest*, *supra* note 128.

130. *See, e.g.*, Murphy, *supra* note 125; *see also* Jacey Fortin, *In Serial Rape Case that Stumped Police, Genealogy Database Leads to Arrest*, N.Y. TIMES (Aug. 23, 2018), https://www.nytimes.com/2018/08/23/us/ramsey-street-rapist-dna.html; *Michella Welch Killing: DNA in Genealogy Database Leads to Man's Arrest in 1986 Cold Case*, INSIDE

enforcement may use the database.[131] Some have recognized the opportunities in this field of investigation. For instance, Parabon Nanolabs was not involved in the Golden State Killer investigation, but the company now offers a service to help law enforcement conduct genetic testing and find a match in open source databases.[132]

The growth of private and open source DNA databases and improvements in DNA technology also have significant implications for how law enforcement may use DNA databases in the future. A recent study found that approximately sixty percent of individuals of European descent could be identified through familial matching in a genetic database.[133] As consumer genetic testing expands, it is likely that nearly all individuals of European descent could be identified through familial matching in consumer DNA databases in the near future.[134] The study also had implications for the identity of individuals within genetic databases. Researchers in the study took a supposedly anonymous DNA sample from a public dataset and uploaded it to GEDmatch.[135] With one day of work, the researchers were able to identify the individual.[136] Separately, another group of researchers

---

EDITION (June 22, 2018, 2:30 PM), https://www.insideedition.com/michella-welch-killing-dna-genealogy-database-leads-mans-arrest-1986-cold-case-44443.

131. *See* Zhang, *supra* note 51 (explaining that the creators of GEDmatch updated its terms of service after learning that law enforcement had used the site in the Golden State Killer investigation); *see also supra* note 121 and accompanying text.

132. *See* Murphy, *supra* note 125 (describing the collaboration between Parabon NanoLabs and the Snohomish and Skagist County Sheriff offices in Washington); *see also* Antonio Regalado & Brian Alexander, *The Citizen Scientist Who Finds Killers from Her Couch*, MIT TECH. REV. (June 22, 2018), https://www.technologyreview.com/s/611529/the-citizen-scientist-who-finds-killers-from-her-couch (noting that the Parabon Nanolabs unit is headed by a TV-famous geneticist).

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

134. *Id.*

135. *Id.* at 692–93. The study specifies individuals of "European descent," defined as Americans of European descent, are currently over-represented in most DNA databases containing consumer testing data. *See* Brian Resnick, *How Your Third Cousin's Ancestry DNA 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. This over-representation of individuals of European descent stands in contrast to most law enforcement-operated DNA databases, where individuals of African and Hispanic descent are over-represented. *See* Brett Mares, *A Chip off the Old Block: Familial DNA Searches and the African American Community*, 29 LAW & INEQ. 395, 407–09 (2011); Daniel J. Grimm, Note, *The Demographics of Genetic Surveillance: Familial DNA Testing and the Hispanic Community*, 107 COLUM. L. REV. 1164, 1175–80 (2007).

136. *Id.* at 693.

determined that it may be possible for law enforcement to use the data from its own databases and compare it against SNP profiles on sites like GEDmatch to identify close relatives.[137] If law enforcement took advantage of this technology, it could rapidly expand the reach of state and federally run DNA databases like CODIS.

D. The Right to Privacy

The police practice of uploading a suspect's DNA to a publicly available website raises significant concerns about whether law enforcement has infringed upon one or more of the suspect's rights.[138] The Supreme Court has established that individuals do have a constitutional right to privacy, even though such a right is not explicitly enumerated within the text of the Constitution. In *Griswold v. Connecticut*,[139] the Court recognized that the Constitution has certain "penumbras" that emanate from other explicitly established rights and give those rights "life and substance."[140] The Court recognized a right to privacy in *Griswold* emanating from the First Amendment's right to association, the Third Amendment's right to exclude soldiers from quartering in the home, the Fourth Amendment's right to be free from unreasonable searches and seizures, and the Fifth Amendment's right to be free from self-incrimination.[141] Additionally, the Court noted that the Ninth Amendment provides that the enumerated rights of the Constitution "shall not be construed to deny or disparage others retained by the people,"[142] and used the Due Process Clause of the Fourteenth Amendment to apply this right of privacy to the states.[143]

The Court's jurisprudence on the right to privacy protects two separate interests: an "individual interest in avoiding disclosure of personal matters" and an "interest in independence in making certain

---

137. Jaehee Kim et al., *Statistical Detection of Relatives Typed with Disjoint Forensic and Biomedical Loci*, 175 CELL 848, 848 (2018).

138. This Comment solely addresses concerns regarding the right to privacy, but there are also important questions about the practice's constitutionality under the Fourth Amendment and the applicability of state laws that disallow familial DNA testing within the state's own databases. *See, e.g.*, Natalie Ram, *Incidental Informants: Police Can Use Genealogy Databases to Help Identify Criminal Relatives—But Should They?*, 51 MD. B.J. 8 (2018).

139. 381 U.S. 479 (1965).

140. *Id.* at 484 (citing Poe v. Ullman, 367 U.S. 497, 516–22 (1961) (Douglas, J., dissenting)).

141. *See id.* (examining the "zones of privacy" created by the Bill of Rights).

142. *Id.* (quoting U.S. CONST. amend. IX).

143. *Id.* at 481–82.

kinds of important decisions."[144] In *Whalen v. Roe*,[145] the Court describes the right to avoid "disclosure of personal matters" as the interest protected by the Court in its *Griswold* decision.[146] In addition to the reasoning in *Griswold*, the Court in *Whalen* also cited Justice Brandeis's dissent in *Olmstead v. United States*[147] as upholding a right to privacy that protects individuals from disclosure of certain personal information.[148] In his *Olmstead* dissent, Justice Brandeis referred to a "right to be let alone," which he asserted was "the right most valued by civilized men."[149]

In dicta, the Court has also recognized certain privacy rights of family members. In *National Archives and Records Administration v. Favish*,[150] the Court stated that the family of a deceased individual has a privacy interest in the details of the deceased's death under both "cultural tradition" and the common law.[151] While the Court ultimately resolved the *Favish* case on procedural grounds, the dicta in this case provides insight into how the Court conceptualizes the privacy rights of family members.[152] Additionally, in the Fourth Amendment context, courts generally recognize that where multiple individuals have a privacy interest, consent of all parties is required to waive a constitutional right.[153]

The Court has stated that an individual does not have a privacy interest in certain areas, most notably in illegal activity.[154] However, in other areas, the Court has acknowledged an expanded privacy interest.

---

144. Whalen v. Roe, 429 U.S. 589, 599–600 (1977). The right to independently make important decisions derives from the privacy interest established in *Roe v. Wade*, which expanded the right to privacy to also include the right of a woman to make a decision regarding abortion, in consultation with her doctor. 410 U.S. 113, 154 (1973). Because this Comment does not concern a private decision made by an individual, but rather a practice used by the government that implicates an individual's privacy rights, this Comment will not discuss this particular branch of privacy rights jurisprudence.

145. 429 U.S. 589 (1977).

146. *Id.* at 599 n.25.

147. 277 U.S. 438 (1928).

148. *Whalen*, 429 U.S. at 599 n.25.

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

150. 541 U.S. 157 (2004).

151. *Id.* at 168–70.

152. *Id.* at 165, 174.

153. *See* Georgia v. Randolph, 547 U.S. 103, 114 (2006) (stating that when a co-tenant objects to a search, even though another co-tenant consents, the objection overrules the consent).

154. *See, e.g.*, Illinois v. Caballes, 543 U.S. 405, 408–09 (2005) ("We have held that any interest in possessing contraband cannot be deemed 'legitimate,' and thus, governmental conduct that *only* reveals the possession of contraband 'compromises no legitimate privacy interest.'" (quoting United States v. Jacobsen, 466 U.S. 109, 123 (1984))).

In recent years, the Court has had to address privacy in the context of a changing world. Technology has drastically changed what information law enforcement can obtain and use in the criminal justice context. This section will address how the Court has handled expansions in technology in the Fourth Amendment context.[155] While this Comment addresses the right to privacy and not Fourth Amendment rights, the Court has explicitly noted that the right to privacy derives in part from the guarantees set forth in the Fourth Amendment.[156] Thus, the privacy interests protected by the Court in the Fourth Amendment context also implicate which interests are protected in the right to privacy context. This section then addresses the right to privacy in the context of the state disclosing sensitive information, particularly sensitive medical information.[157]

1. Privacy and technology

In addition to famously recognizing the "right to be let alone," Justice Brandeis's dissent in *Olmstead* also warned that as technology develops, the "progress of science" could provide the government with more ways to violate the Fourth Amendment rights of its citizens.[158] As modern technology has developed, the Supreme Court has increasingly extended privacy rights to cover the privacy invasions presented by new technology.[159] In the Fourth Amendment context, the Supreme Court has expanded protections to cell phone location data provided to a third party, examining the contents of a cell phone, and scanning an individual's home with a heat sensor.[160]

In deciding each of these cases, the Supreme Court found that changes in technology—and the way that the technology is commonly used in society—can change how "private" society perceives the information. For instance, in *Riley v. California*,[161] the Court noted that smartphones are now an integral part of most adults' daily lives in a way that cell phones

155. *See infra* Section I.D.1.

156. Griswold v. Connecticut, 381 U.S. 479, 484–86 (1965).

157. *See infra* Section I.D.2.

158. Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

159. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (cell phone tracking data); Kyllo v. United States, 533 U.S. 27, 40 (2001) (heat sensors); Katz v. United States, 389 U.S. 347, 358 (1967) (recording device in phone booth).

160. *See Carpenter*, 138 S. Ct. at 2223; Riley v. California, 134 S. Ct. 2473, 2494–95 (2014); *Kyllo*, 533 U.S. at 40–41.

161. 134 S. Ct. 2473 (2014).

were not just a couple decades ago.[162] Similarly, in *Kyllo v. United States*,[163] the Court found that while law enforcement may legally observe a home from a public street, enhancing the senses through the use of a heat detector was an impermissible invasion of privacy which required a warrant.[164] Taken together, these Fourth Amendment cases demonstrate that constitutional rights are interpreted in the context of modern technology, particularly where that technology presents a further invasion into the intimate parts of an individual's life.[165]

2. Privacy and DNA

The Supreme Court has thus far not dealt extensively with how expanding technology use applies in the context of DNA analysis. In one of only a handful of cases addressing DNA, *King*,[166] the Court held that law enforcement may take DNA from an individual arrested for a crime.[167] However, in *King*, the Court focused on the physical taking of the DNA itself via a buccal swab of the arrestee's mouth as the "search" within the context of the Fourth Amendment, not the later DNA testing and analysis of that swab.[168] The Court also recognized that the DNA sample taken from the arrestee would only be used to establish the arrestee's identity, not to explore further data that could potentially be revealed through DNA testing.[169]

While some state courts have found that a DNA test is a search separate from the search collecting the DNA sample, federal courts have followed the reasoning set forth by the Court in *King*.[170] Some lower federal courts have reasoned that because suspects of crime do not have privacy rights to their identity, and traditional DNA testing used by law enforcement only reveals information related to a suspect's identity, DNA testing is not a search for the purposes of the Fourth

---

162. *Id.* at 2484.
163. 533 U.S. 27 (2001).
164. *Id.* at 34–36.
165. *See Riley*, 134 S. Ct. at 2484–85 (examining how to interpret modern cell phone use by balancing government interests against the degree of privacy intrusion).
166. 569 U.S. 435 (2013).
167. *Id.* at 465–66.
168. *Id.* at 446.
169. *See id.* at 450–51 (equating the practice of using DNA swabs with the common practices of using wanted posters, tattoos, or fingerprints to identify an arrestee).
170. *Compare* Patterson v. State, 742 N.E.2d 4, 9 (Ind. Ct. App. 2000) (holding that a DNA test is a separate search), *with* Boroian v. Mueller, 616 F.3d 60, 67–68 (1st Cir. 2010) (holding that testing a DNA sample is not a separate search under the Fourth Amendment).

Amendment.[171] Because law enforcement use of SNP testing is relatively new and has not yet faced legal challenges, courts have not ruled on how this more sophisticated and revealing form of DNA testing applies in the privacy or Fourth Amendment context.[172]

3. Privacy and medical information

The Supreme Court has not specifically ruled upon the issue of public officials releasing private genetic information about a suspect.[173] However, precedent from the Court sheds light on how it conceptualizes government use of personal medical information. Additionally, lower court decisions regarding the release of medical information of prisoners present an analogue for how courts may conceptualize the release of an individual's DNA data. While the Court acknowledges in many of the cases noted in this section that an individual has a reduced expectation of privacy in certain situations, the Court does not state in any case that a right is wholly inapplicable to a particular individual. This is because an individual still retains his constitutional rights even when he has a reduced expectation of privacy.[174]

The Supreme Court jurisprudence regarding drug testing sheds light on how the Court handles cases where private information about an individual may be revealed through testing of bodily fluids. Generally, the Court has been more permissive of testing in situations where the individual has a reduced expectation of privacy or where the

171. *See Boroian*, 616 F.3d at 66 ("CODIS currently functions much like a traditional fingerprint database, permitting law enforcement to match one identification record against others contained in the database."); Johnson v. Quander, 440 F.3d 489, 499 (D.C. Cir. 2006) (comparing CODIS to an "old-fashioned fingerprint database" used only for identifying individuals).

172. *See generally* Matt Ford, *How the Supreme Court Could Rewrite the Rules for DNA Searches*, NEW REPUBLIC (Apr. 30, 2018), https://newrepublic.com/article/148170/supreme-court-rewrite-rules-dna-searches (discussing how this new police practice of uploading DNA could change the Supreme Court's DNA jurisprudence).

173. The closest case analogous to police releasing private information about a suspect is *Wilson v. Layne*, 526 U.S. 603 (1999), in which the Court held that police had violated an individual's Fourth Amendment rights by bringing members of the media along while police executed a search warrant in an individual's home. *Id.* at 614. However, this decision was limited and based heavily on the facts of the case at hand and did not prevent the media from joining law enforcement during the execution of a search warrant in all situations. *Id.*

174. *See* Winston v. Lee, 470 U.S. 753, 758–60 (1985) (discussing a suspect's Fourth Amendment rights, which the suspect retains despite a reduced expectation of privacy).

test is less invasive.[175] In *Vernonia School District 47J v. Acton*,[176] a case challenging a school district's policy of drug-testing student athletes, the Court found for the school district, reasoning that the school's custodial relationship with the students and the students' diminished expectation of privacy at school made the drug testing policy reasonable under the Fourth Amendment.[177] The Court also found for the government in a case challenging a Federal Railroad Administration regulation that permitted drug testing of railroad employees.[178] In *Skinner v. Railway Labor Executives Ass'n*,[179] the Court recognized that the compelling interest in ensuring that employees were drug-free outweighed the potential intrusion on the employees' privacy.[180] However, in a case involving breath testing and blood testing of drunk drivers during the course of arrest, the Court permitted the state to use breath testing during a search incident to arrest but required a warrant for a blood test due to the invasive nature of the testing.[181]

The Court has implicitly acknowledged that the government releasing private medical information about individuals may implicate a privacy right. In *Whalen*, the Supreme Court addressed the issue of the state compelling pharmacies to track purchases of otherwise legal drugs.[182] The Court recognized a compelling state interest in tracking legal sales of drugs that may be used to make illegal substances.[183] Ultimately, the

---

175. The Court has recognized that individuals have a reduced expectation of privacy in a number of contexts, including when an individual shares information with a third party, when an individual is a student at a public school, when an individual is operating a vehicle, and when an individual is arrested for a crime. *See* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) (third parties); Maryland v. King, 569 U.S. 435, 463 (2013) (arrestees); Wyoming v. Houghton, 526 U.S. 295, 303 (1999) (vehicle passengers and drivers); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 657 (1995) (student athletes). Additionally, the Court has found that an individual does not have a privacy right in "abandoned" items or items exposed to public view. *See* California v. Greenwood, 486 U.S. 35, 40–41 (1988) (trash exposed to public not protected by privacy rights); Massachusetts v. Painten, 389 U.S. 560, 566 (1968) (White, J., dissenting) ("Of course 'abandoned' property may be seized . . . .").

176. 515 U.S. 646 (1995).

177. *Vernonia Sch. Dist. 47J*, 515 U.S. at 656–57.

178. Skinner v. Railway Labor Executives Ass'n, 489 U.S. 602, 606 (1989).

179. 489 U.S. 602 (1989).

180. *Id.* at 624.

181. *See* Birchfield v. North Dakota, 136 S. Ct. 2160, 2185 (2016) ("Because breath tests are significantly less intrusive than blood tests and in most cases amply serve law enforcement interests, we conclude that a breath test, *but not a blood test*, may be administered as a search incident to a lawful arrest for drunk driving." (emphasis added)).

182. 429 U.S. 589, 591 (1977).

183. *Id.* at 597–98.

Court ruled in favor of the state, but acknowledged that the state computer files used to store the data were vulnerable, and declined to rule on any questions regarding the "disclosure of accumulated private data," whether such disclosure was "intentional or unintentional."[184]

One area where lower courts have recognized a privacy interest is in the disclosure of a prisoner's HIV or transgender status. For example, in 1994 the United States Court of Appeals for the Second Circuit first recognized a prisoner's privacy interest in HIV status in *Doe v. City of New York*.[185] The Second Circuit later addressed that same right in *Powell v. Schriver*,[186] holding that a prisoner, while deprived of many constitutional freedoms when incarcerated, nonetheless retains a right to privacy in her HIV and transgender status.[187] Although the Second Circuit ultimately found that the government officials had qualified immunity for the release of information about the prisoner in *Powell*, the court acknowledged that a prisoner has some privacy interest in her HIV and transgender status that may remain protected even while she is incarcerated.[188] Other federal courts have also found disclosures of a prisoner's HIV status to violate a prisoner's right to privacy in his medical information, although most of these cases also resulted in qualified immunity for the prison officials.[189]

Taken together, these cases indicate that while a diminished expectation of privacy in certain information can permit the government to collect certain personal information, the invasiveness of the testing process matters when analyzing the privacy interests of an individual. The cases concerning medical information build upon this rule by establishing that even in situations where an individual has a reduced expectation of privacy, such as in the case of imprisoned individuals, an individual retains

184. *Id.* at 605–06.

185. 15 F.3d 264 (2d Cir. 1994).

186. 175 F.3d 107 (2d Cir. 1999).

187. *See id.* at 111–13 (accepting that the right to privacy in medical information exists for incarcerated prisoners, but explaining that such a right may be impinged if related to a legitimate penological interest, but not if used as humor or gossip).

188. *Id.* at 113–14.

189. *See* Herring v. Keenan, 218 F.3d 1171, 1175, 1180 (10th Cir. 2000) (finding that disclosure of HIV status was a violation of a constitutional right, but offering qualified immunity because the right was not yet clearly defined); *Doe*, 15 F.3d at 267 (recognizing that there is a right to "confidentiality" that is distinguishable from right to autonomy and decision making, and finding that this right is violated by disclosing confidential information such as a prisoner's HIV status); *see also* Doe v. Delie, 257 F.3d 309, 317–18 (3d Cir. 2001) (finding that prison officials had qualified immunity, but recognizing that a prisoner has a privacy interest in his HIV status).

at least some privacy interest which protects against the release of sensitive information to outside parties. Part II of this Comment addresses these rules in the context of law enforcement uploading the results of an invasive DNA test to a public website.

II. ANALYSIS

As established in the previous sections, modern DNA testing allows law enforcement to learn far more information about an individual than simply the individual's identity. This Comment argues that a suspect and his blood relatives have a right to privacy in the DNA data that goes beyond the individual's identity to sensitive traits, and that law enforcement violates this privacy right by uploading the data to a public DNA database. This section will first explore how this law enforcement practice violates the right to privacy of the suspect himself by releasing sensitive information, particularly medical information, about the suspect.[190] This section will then address the privacy rights implications of this practice on individuals related to the suspect, whose medical history may also be disclosed through the uploading of a relative's genetic data.[191] Ultimately, this section will argue that because innocent third parties who are related to the suspect do not have a diminished expectation in their privacy, the practice of uploading a relative's DNA violates the family's right to privacy in their own genetic data because the family members share DNA with the suspect.[192]

A. The Suspect's Right to Privacy

When an individual is suspected of a crime and not yet convicted, he retains the rights guaranteed under the U.S. Constitution.[193] While the Supreme Court has recognized that there are areas and circumstances that reduce an individual's right to privacy,[194] these circumstances do not extinguish this right entirely.[195] However, in the context of investigating an unknown DNA sample, the "suspect" and his rights are difficult to

190. *See infra* Section II.A.

191. *See infra* Section II.B.

192. *See infra* Section II.B.

193. *See, e.g.*, Winston v. Lee, 470 U.S. 753, 758–60 (1985) (discussing the suspect's right to be free of unreasonable searches and seizures under the Fourth Amendment, a right which the Court assumes the suspect retains even while suspected of a crime).

194. *See* Birchfield v. North Dakota, 136 S. Ct. 2160, 2177 (2016) (stating that arrest necessarily diminishes the privacy expectations of the individual).

195. *See* Doe v. Delie, 257 F.3d 309, 316–17 (3d Cir. 2001) (finding that incarcerated individuals retain some rights to privacy, although those rights may be subject to limitations).

define, as the individual has not yet been identified by law enforcement. Law enforcement certainly has a compelling interest in finding the identity of that individual, but even compelling state interests have certain limits.[196] In the sections that follow, this Comment argues that a suspect has a privacy interest in the intimate information contained within sophisticated DNA test results, and that law enforcement violates this right to privacy by uploading the DNA data to a public website where an unknown number of users could obtain the data.

1. Modern technology

As discussed above, an individual's DNA contains a vast amount of information because DNA is the "blueprint" for the human body to make the proteins that define how an individual's body looks and functions.[197] The amount of information revealed by a DNA test, however, is dependent on the type of DNA test that is performed on the DNA sample.[198] A DNA test could solely target non-coding regions of DNA, which would help establish a code that can be compared for identity purposes with another DNA sample, but would not be useful in establishing any further information about the individual.[199] A more sophisticated DNA test, such as an SNP test, could reveal far more information, establishing not only a code that informs the tester of an individual's identity, but also reveals sensitive information about the individual, such as race, ethnicity, or potential to develop a number of different genetically-linked diseases.[200]

Advances in technology can greatly impact how courts perceive a violation of privacy rights.[201] Something that previously held only some personal data, such as a cell phone's location, can rapidly become far more significant in daily life and therefore present an area where society recognizes a privacy interest, even if there may not have been a privacy interest in that area before.[202] Thus, while DNA testing has been less intrusive in the past, modern technology permits law enforcement to intrude far more into a suspect's medical and genetic

196. *See, e.g.*, *supra* notes 185–89 and accompanying text (discussing that a prisoner has a privacy interest in his HIV status which overrides the state interest in his HIV status).
197. *See* CUTICCHIA *supra* note 26 and accompanying text.
198. *See supra* Section I.A.2.
199. *See supra* notes 50–53 and accompanying text.
200. *See supra* notes 54–56 and accompanying text.
201. *See supra* notes 158–65 and accompanying text.
202. *See* Carpenter v. United States, 138 S. Ct. 2206, 2216–19 (2018).

information than ever before.[203] Some of these SNP tests can reveal medical information, such as a risk for breast cancer, Parkinson's disease, and diabetes, all of which may be linked to certain genetic traits.[204] Additionally, even a basic DNA test can reveal the sex of an individual at birth.[205] Given that the Second Circuit has already recognized a right to confidentiality with regard to an individual's transgender identity, releasing information from a DNA sample could violate an individual's right to privacy by releasing sensitive information about his gender identity.[206]

In *Carpenter* and *Riley*, the Supreme Court also recognized that cell phone technology will only continue to become more sophisticated in the future.[207] The Court recognized that as cell phone technology becomes more integrated into people's lives, the more sensitive information can be revealed by a search of the phone.[208] In *Carpenter*, the Court explicitly stated that its ruling would only become more important as the ability to pinpoint an individual's location via his cell phone becomes more sophisticated.[209] The same is true for hackers targeting websites.[210] As companies develop new ways to protect information, individuals who seek to gain access learn new ways to unlawfully obtain the information.[211] Additionally, a recent study

---

203. *See* Justin Jouvenal, *The Unlikely Crime-Fighter Cracking Decades-Old Murders? A Genealogist.*, WASH. POST (July 16, 2018), https://www.washingtonpost.com/local/public-safety/in-decades-old-crimes-considered-all-but-unsolvable-genetic-genealogy-brings-flurry-of-arrests/2018/07/16/241f0e6a-68f6-11e8-bf8c-f9ed2e672adf (noting that modern DNA testing websites, such as GEDmatch, have DNA profiles containing over 600,000 SNPs, allowing users "not only to identify a match but also to determine how closely people are related").

204. *See* Saey, *supra* note 56 (discussing the health information provided by 23andMe and other online DNA testing services).

205. *See* CUTICCHIA, *supra* note 26, at 8 (illustrating that biological males have XY chromosomes, while biological females have XX chromosomes).

206. *See* Powell v. Schriver, 175 F.3d 107, 111–12 (2d Cir. 1999) (concluding that a prisoner has the right to maintain privacy in her "transsexual" and HIV status while incarcerated, subject only to "legitimate penological interests").

207. *Carpenter*, 138 S. Ct. at 2218; Riley v. California, 134 S. Ct. 2473, 2484–85 (2014).

208. *Carpenter*, 138 S. Ct. at 2218; *Riley*, 134 S. Ct. at 2485.

209. *Carpenter*, 138 S. Ct. at 2219.

210. *See* Nick Miroff, *Hacking, Cyberattacks Now the Biggest Threat to U.S., Trump's Homeland Security Chief Warns*, WASH. POST (Sept. 5, 2018), https://www.washingtonpost.com/world/national-security/hacking-cyberattacks-now-the-biggest-threat-to-us-trumps-homeland-security-chief-warns/2018/09/05/d0045800-b119-11e8-a20b-5f4f84429666 (discussing the threat of hacking in the national security context).

211. *See, e.g.*, Angela Chen, *Why a DNA Data Breach Is Much Worse Than a Credit Card Leak*, VERGE (June 6, 2018, 3:54 PM), https://www.theverge.com/2018/6/6/1743

indicates that it is possible, with some knowledge and expertise, for an outside individual to identify a previously "anonymous" set of genetic data.[212] This indicates that if law enforcement can use a pubic database to identify a suspect, citizen sleuths may be able to in turn identify which set of genetic data belongs to a particular suspect, even if law enforcement attempted to conceal the identity of the suspect when uploading the DNA to a public website.

In a DNA database operated by law enforcement, there are protocols regarding how DNA is tested, who can test the DNA, and who has access to the information stored in the database.[213] Law enforcement databases are used to solve crimes and are not available to the general public.[214] Thus, while an individual cannot know for sure who is accessing his DNA stored in a law enforcement database, he can generally be sure that the information will only be viewed by authorized officials. However, when law enforcement turns over a suspect's DNA data to a public open source DNA database such as GEDmatch, it turns over all of its ability to control who may have access to that information. Even though law enforcement may make its best effort to keep the data it uploads anonymous, it has no means of knowing if the data will be kept anonymous in the future. The protections regarding access and accountability that are established by statute in the case of state and federal DNA databases are simply not present in the world of open source data.

Advances in DNA technology, coupled with the rise of online DNA databases, allow law enforcement to obtain more sensitive data about a suspect than ever before. Yet, once law enforcement uploads a suspect's DNA information to a public DNA website, they have little control over how the data is used or who may access it. However, if a suspect has no privacy right in the genetic information released by law enforcement, then there would be no violation of the suspect's rights. The next section explores why a suspect has a privacy right in the genetic information uploaded by law enforcement.

5166/myheritage-dna-breach-genetic-privacy-bioethics (discussing a breach of 92 million user accounts on a DNA database website).

212. *See* Yaniv Erlich et al., *Identity Inference of Genomic Data Using Long-Range Familial Searches*, 362 SCI. 690, 692–93 (2018) (finding that scientists could identify a previously anonymous individual by searching genetic data GEDmatch and using public records).

213. *See supra* Section I.B.1 (describing the requirements for testing DNA to include the sample in federal databases).

214. *See CODIS and NDIS FAQs*, *supra* note 64 (stating that "[a]ccess is restricted to criminal justice agencies for law enforcement identification purposes").

2. A privacy interest in DNA test results

As discussed above, the technologies used to test DNA in preparation for uploading to GEDmatch are far more intrusive than the other forms of DNA testing used by law enforcement and go far beyond simply assisting law enforcement in identifying a suspect.[215] To prepare a DNA sample to be uploaded to a genetic database, law enforcement must test the DNA in a manner akin to that of private, direct-to-consumer companies like Ancestry or 23andMe.[216] The DNA loci used in this kind of SNP testing can reveal far more information than the traditional DNA tests run by law enforcement for inclusion in CODIS.[217] Exactly what tests law enforcement uses in preparation for uploading a DNA profile to a public website, and exactly which loci are used in the testing process, have not been publicly disclosed. Thus, DNA testing done by law enforcement when preparing to upload a DNA profile to an open source database can potentially reveal sensitive medical information. Due to a lack of law enforcement transparency, the extent of the information revealed by that test may be difficult for the public to determine.[218] However, even without knowing the full panel of loci used by law enforcement,[219] this more invasive DNA test would necessarily include information regarding the individual's ancestry, and potentially information relating to genetically-linked diseases as well.[220] This is in stark contrast to how law enforcement uses its own databases, where the DNA must be tested in a manner clearly delineated and made publicly available by federal agencies.[221] Additionally, the DNA loci tested by law enforcement for inclusion in a law enforcement database do not test for any sensitive information.[222]

The privacy interests in information protected by the federal courts are analogous to the information at risk of disclosure when law enforcement uploads DNA data to a public website. In *Doe* and *Powell*,

---

215. *See supra* notes 54–56 (discussing the data collected in SNP testing).

216. *See supra* notes 69–75 and accompanying text.

217. *See supra* notes 54–56 and accompanying text.

218. In contrast, CODIS's website explicitly states which loci are used in the testing process for inclusion in the DNA index. *See CODIS and NDIS FAQs*, *supra* note 64.

219. *See Parabon Snapshot*, PARABON NANOLABS, https://snapshot.parabon-nanolabs.com/#genealogy-how (last visited Feb. 5, 2019) (describing a service for law enforcement that provides SNP testing for DNA samples, but not disclosing which loci are used).

220. 23ANDME, *supra* note 96.

221. *See CODIS and NDIS FAQs*, *supra* note 64 (describing the process for testing and storing DNA in federal databases).

222. *See supra* notes 72–73 and accompanying text.

the Second Circuit recognized privacy interests of prisoners who were HIV positive.[223] The Second Circuit in *Doe* reasoned that the right to privacy extended to "information about the state of one's health."[224] The Second Circuit further recognized the stigma of HIV and transgender status and the potential for harassment or harm if that information released publicly in its decision in *Powell*.[225] While DNA testing cannot definitively state that an individual will get a particular disease, it can establish that the individual has a higher likelihood of developing such a disease.[226] Thus, under the reasoning of *Doe* and *Powell*, the individual has a privacy interest in that sensitive health information and should be permitted, within reason, to control when and to whom that information is disclosed.

While the government is permitted to possess sensitive information, this does not mean the government may freely release that information to the public. In *Whalen*, the Supreme Court recognized that the state government may mandate the disclosure to the state's Department of Health of which individuals had been prescribed Schedule II substances.[227] The Court reasoned that despite the appellees' assertion that the data was insecure, there was no reason for the "assumption that the security provisions of the statute will be administered improperly."[228] However, the law enforcement practice of uploading a suspect's DNA data to a public website is an explicit release of the suspect's information. The entire practice is predicated on the release of the information, instead of a potential incidental effect of collecting the data. Thus, while law enforcement may have a right to test the crime scene DNA to collect additional data,[229] the subsequent public release of that data would violate the suspect's right to privacy.

A diminished privacy interest in some data does not give law enforcement a blanket license to release whatever information they want in pursuit of finding a suspect. In the school drug-testing case,

---

223. *See supra* notes 185–88 and accompanying text (discussing *Doe* and *Powell*).

224. 15 F.3d 264, 267 (2d Cir. 1994).

225. Powell v. Schriver, 175 F.3d 107, 115 (2d Cir. 1999) (acknowledging dangers of releasing HIV and transgender status in discussion of Eighth Amendment rights).

226. *See* Saey, *supra* note 56 (indicating that DNA testing can reveal increased risk of Alzheimer's, Parkinson's disease, or breast cancer).

227. Whalen v. Roe, 429 U.S. 589, 598–602 (1977).

228. *Id.* at 600, 601.

229. *Supra* notes 166–69 and accompanying text. For an argument that a suspect should retain privacy rights in DNA shed at crime scenes, see David Gusella, Note, *No Cilia Left Behind: Analyzing the Privacy Rights in Routinely Shed DNA Found at Crime Scenes*, 54 B.C. L. REV. 789 (2013).

Vernonia School District 47J v. Acton, the Court's analysis of the students' privacy interest relied in part on what the testing itself revealed.[230] The Court stated that the drug testing procedure revealed only whether or not the student had used illegal drugs, and not whether the student was "for example, epileptic, pregnant, or diabetic."[231] Similarly, in *Skinner*, a case concerning drug testing of public employees, the Court recognized that the urine testing may reveal medical facts about the individual, but nonetheless permitted the practice based on the need to test for drugs quickly and the dire consequences of allowing individuals under the influence of drugs operate railway equipment.[232] The privacy interest at risk in the uploading of a DNA test is distinguishable from these instances. While an individual who has committed a crime does not have a privacy right in his illegal activity,[233] this does not preclude the individual from having a privacy right in other areas of his life. Unlike in *Vernonia School District*, where the testing only revealed the illegal activity of the students, the testing performed by law enforcement may reveal extensive information outside of law enforcement's intended purpose to identify the suspect.[234] Additionally, the purpose of the drug-testing policy in *Skinner* was to prevent railway accidents.[235] However, in the case of crime scene DNA, the crime and the harm has already occurred. While law enforcement certainly has an interest in identifying a suspect as soon as possible, the courts may be more inclined to impose procedural safeguards in this instance.

Some may argue that the suspect, by leaving his DNA at the scene of a crime, has effectively "abandoned" the DNA sample or exposed the sample to the public and therefore does not retain any privacy interest in the DNA sample at all. While some states and lower federal courts have recognized this reasoning as the rule,[236] the Supreme Court has not definitively answered whether a suspect releases all privacy in DNA shed at a crime scene. In addition, the reasoning behind the Court's decision in *Greenwood*, which concerned trash in public view on the street, was that an individual's trash is available and accessible to the

230. *See* 515 U.S. 646, 658 (1995).
231. *Id.*
232. Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 617, 619–21 (1989); *see also supra* notes 178–80 and accompanying text.
233. *See* Illinois v. Caballes, 543 U.S. 405, 408–09 (2005).
234. *See supra* notes 54–56, 125–29.
235. *Skinner*, 489 U.S. at 620.
236. *See supra* note 128.

public once placed curbside.[237] While a DNA sample may be left behind, the information contained within the DNA sample is not readily viewable by the public and requires a significant amount of scientific testing which the average member of the public does not have access to. Additionally, SNP testing on a large commercial scale is a relatively recent occurrence.[238] The fact that the loci used by law enforcement do not reveal any sensitive information about the suspect has been noted in some courts' opinions on the abandonment issue as part of the court's reasoning in permitting the practice of testing "abandoned" DNA.[239] In this evolving area of technology, the Court's precedents may not hold in the face of such invasive use of DNA testing technology.

Additionally, the practice of testing an individual's DNA may lead to stigma or discrimination of other kinds. SNP testing can reveal very specific information about an individual's race and ancestral national origin.[240] This potentially opens the door for law enforcement officers to unfairly stereotype or profile individuals based on a suspect's genetic profile.

An individual has a privacy interest in his medical information, and SNP testing is capable of revealing such information. While law enforcement may permissibly run such a genetic test on DNA found at a crime scene because of the suspect's reduced expectation of privacy, law enforcement cannot upload the data to a public website without violating the privacy rights of the individual to whom the DNA belongs. Once uploaded, law enforcement loses all ability to control who may have access to that data and potentially shares sensitive genetic information about a suspect with the public.

B. The Suspect's Family's Right to Privacy

In addition to the suspect's right to privacy in his own genetic material, the process of uploading a suspect's DNA may also implicate members of his family. This section first describes the implications of the unavoidable sharing of DNA between family members,[241] and then argues that the family members' privacy rights in their own genetic material is violated when law enforcement uploads the genetic testing data of a relative.[242]

---

237. 486 U.S. 35, 40–41 (1988).

238. *See supra* notes 97–111 and accompanying text.

239. *See, e.g.*, Raynor v. State, 99 A.3d 753, 755 (Md. 2014) (finding that the testing of "13 identifying 'junk' loci," without a physical intrusion on the body, was not a search under the Fourth Amendment).

240. *See supra* notes 54–56 and accompanying text.

241. *See infra* Section II.B.1.

242. *See infra* Section II.B.2.

1. Shared DNA between biologically related individuals

As noted above, related individuals can share a significant amount of the same DNA.[243] Parents and children share exactly half of the same DNA, and close relatives share a substantial percentage of the same DNA as well.[244] Thus, knowing the genetic background of one individual can implicate the genetic background of his close relatives. Additionally, some medical diseases often run in families and are genetically linked.[245] An individual's likelihood of getting these genetically-linked diseases can be detected by testing DNA.[246]

In the context of uploading a suspect's DNA to a public website, law enforcement must also find a match to one of the suspect's genetic relatives in order to trace the suspect's family tree.[247] These genetic relatives have made an active choice to upload their own DNA profiles to an open source website, functionally placing their genetic information in "public view" and, thus, opening their DNA profile to police scrutiny under the reasoning of *Greenwood*.[248] However, after matching a suspect's DNA to a genetic relative, law enforcement will use public records to investigate the known match's family tree and identify the suspect.[249] While currently an opaque process, this would likely involve law enforcement identifying many other individuals related to the suspect, including close relatives such as parents or children of the suspect.[250] These other genetic relatives may have never openly released their DNA to public or law enforcement scrutiny. The consent of the genetic relative who uploaded his DNA sample cannot also be used as consent for all members of his family to release information about the family genetic line.[251] Nevertheless, this may allow law enforcement to obtain sensitive information about the relative's genetic makeup, by virtue of analyzing the genetic makeup of the suspect, without ever possessing the relative's DNA.

---

243. *See supra* notes 88–89 and accompanying text (discussing the average amount of DNA shared between relatives).

244. *See supra* notes 88–89 and accompanying text.

245. *See* Saey, *supra* note 56 (explaining how genetic testing can reveal likelihood of breast cancer).

246. *Id.*

247. *See supra* notes 125–26 and accompanying text.

248. *See supra* notes 112–16.

249. *See supra* note 125 and accompanying text.

250. *See supra* note 125 and accompanying text.

251. *Cf.* Georgia v. Randolph, 547 U.S. 103, 114–15 (2006) (finding in the Fourth Amendment context that one occupant of a home may not give consent for a search if another occupant is present and objecting to the search).

Additionally, as law enforcement uses the practice of uploading a suspect's DNA to a publicly available database grows, questions of consent become even further complicated. It is unclear right now whether law enforcement deletes the DNA information of the suspect from the public database once law enforcement has obtained the familial information it needs to identify the suspect. If law enforcement leaves the suspect's genetic profile on the public database, then that profile becomes public information for other law enforcement agencies to search when looking for a suspect. If a second law enforcement agency makes an arrest based on genetic information uploaded by the first law enforcement agency that the suspect never consented to making public, the same consent argument noted above would not hold. Should this practice become commonplace, the further use of uploaded genetic information for other purposes is an important consideration for law enforcement.

2. Privacy rights of innocent third parties

Relatives of a criminal suspect do not give up their privacy rights simply because of a genetic link to the suspect. Thus, innocent third parties do not have a diminished expectation of privacy in their genetic data in the same way that someone who has committed an illegal act would.[252] In most other instances, such as drug-testing or revealing an individual's HIV status, the information is generally specific to one person and does not implicate any outside parties. However, this is not the case in the context of genetic material. Knowing that a woman has a genetic marker that increases risk for breast cancer, for instance, necessarily indicates that her daughter may have inherited the same gene.[253]

While not every relative will share every trait with the suspect, the implication of shared genetic material alone could be enough to damage the reputation of a related individual. In *Favish*, the Supreme Court recognized a family's privacy interest in information about a deceased relative.[254] The family members in *Favish* sought to protect their own interests in securing "refuge from a sensation-seeking

252. *See supra* Section II.A; *cf.* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 665 (1995) (stating that while the Court upheld suspicionless drug testing in some situations, it would likely not permit suspicionless searches in circumstance where the individuals being searched did not have a diminished expectation of privacy).

253. *See Genetics*, BREASTCANCER.ORG, https://www.breastcancer.org/risk/factors/genetics (last visited Feb. 5, 2019) (asserting that "[a]bout 5% to 10% of breast cancers are thought to be hereditary, . . . passed from parent to child").

254. 541 U.S. 157, 168–69 (2004).

culture for their own peace of mind and tranquility."[255] While the Court ultimately drew its conclusions regarding privacy in *Favish* from the text of the statute, the Court also recognized that intrusions on these privacy rights were "long deemed impermissible under the common law and in our cultural traditions."[256] *Favish* indicates that family members, in a situation where public pressure is applied to them based on the actions of a related individual, have a privacy right in protecting their lives from outside scrutiny.[257] When officers release an individual's DNA to the public, they invite scrutiny of those closely related to the accused in one of the most sensitive ways possible by revealing information that may bear on the family's collective medical history.

Thus, when law enforcement uploads a suspect's DNA to a public open source DNA database, law enforcement also reveals information regarding the suspect's relatives.[258] Because the privacy rights of innocent family members not suspected of a crime are not tempered by any diminished expectation of privacy, the release of this information violates a privacy right in the relatives' genetic data.

CONCLUSION

DNA testing technology has grown vastly more sophisticated in recent years, and law enforcement has chosen to use this newly available technology to track down suspects in cold cases. Additionally, given the success of this technology in solving cold cases, law enforcement may decide to use this technology in more types of cases. While the goal of bringing criminals to justice is certainly laudable, law enforcement must exercise caution when using open source DNA databases and not abuse the powerful information that it can now obtain. The technology used by law enforcement currently presents a significant intrusion into not only the potential suspect's right to privacy, but the right to privacy of individuals related to him as well. Uploading a suspect's genetic information to a website that cannot guarantee privacy of that data is a violation of both the suspect's right to privacy in his medical information as well as the right to privacy of individuals related to that suspect.

---

255. *Id.* at 166.
256. *Id.* at 167.
257. *Id.*
258. *See supra* notes 39–42 and accompanying text (discussing the amount of genetic information shared between biologically related individuals).