23POLICEMENANDME: ANALYZING THE CONSTITUTIONAL IMPLICATIONS OF POLICE USE OF COMMERCIAL DNA DATABASES

Evan Frohman[*]

INTRODUCTION

In 1984, the English scientist Alec Jeffery discovered the variable DNA markers that exist within every person.[1] Within a year, the English police became the first law enforcement agency to use DNA's identification capabilities to successfully catch a criminal.[2] The technique crossed the pond to the United States and was soon followed by the creation of a national DNA profile database in 1990.[3] At first, the database was just for sex offenders. Then it was for all felons, then convicted criminals, and now even arrestees.[4] Additionally, some local DNA databases, which lack the regulations and restrictions that federal law imposes on the national database, include witnesses, victims, family members of victims, and helpful citizens who responded to DNA dragnets.[5] This power creep has continued as law enforcement agencies expand the DNA identification technique's reach ever further with the implementation of familial searches, which capture individuals with genetic relation to a DNA profile in the database.[6]

---

* J.D. 2020, University of Pennsylvania Carey Law School; B.A. Political Science, Legal Studies, Economics, 2016, Northwestern University. Special thanks to Professor David Rudovsky, Dr. Stella Tsirka, Dr. Michael Frohman, (soon to be Dr.) Maddie O'Brien, and the University of Pennsylvania Journal of Constitutional Law for their support and wisdom. Sorry Mom, this is the closest I'm getting to science.

1 *The History of Genetic Fingerprinting*, U. OF LEICESTER, https://www2.le.ac.uk/departments/genetics/jeffreys/history-gf (last visited Mar. 7, 2019) (documenting the discovery of DNA).

2 *Id.*

3 David H. Kaye, *The Genealogy Detectives: A Constitutional Analysis of "Familial Searching"*, 50 AM. CRIM. L. REV. 109, 123-24 (2013).

4 Jason Kreag, *Going Local: The Fragmentation of Genetic Surveillance*, 95 B.U. L. REV. 1491, 1527 (2015).

5 Kaye, *supra* note 3, at 111.

6 *Id.* Power creep is when a technology becomes increasingly powerful over time. In the present instance, the speed, accuracy, cost effectiveness, breadth of use, and ability to analyze DNA has drastically increased since 1985.

While commentators have begun confronting the constitutional and public policy implications of DNA profile databases[7] and familial searches,[8] new titans of DNA storage have emerged: commercial DNA databases. Companies such as 23andMe and Ancestry have vast DNA banks collected from individuals voluntarily for non-law enforcement purposes. By April 2020, 23andMe and Ancestry had roughly 10 and 16 million customers, respectively.[9] Smaller companies such as MyHeritage, Family Tree DNA, National Geographic, and many others only add to this monumental resource.[10] The incredible number of DNA profiles in these databases combined with the new familial search technique could subject vast amounts of the American populace to genetic surveillance. Indeed, these companies have already been subpoenaed on multiple occasions by law enforcement and in some cases have already volunteered to work with them.[11]

In what follows, this comment will explore the constitutional and privacy issues surrounding commercial DNA databases, ultimately concluding that despite the Supreme Court's narrowing of the third-party doctrine, it should not be unconstitutional for law enforcement to use the genetic profiles in commercial databases without a warrant, though the companies might have a colorable argument for requiring a pre-compliance review before producing any records. Part I of this comment will describe the science behind DNA testing and familial searches and the structure of the federal DNA database. Part II will examine the constitutionality of DNA databases and searches as well as the constitutionality of familial searches, ultimately concluding that both pass constitutional muster. Part III will discuss the factual and legal framework needed to analyze commercial DNA databases. Part IV will analyze the constitutionality and practicality of police use of commercial DNA databases. Finally, this comment will conclude with the potential implications of

---

7 *Id.*

8 Sonia M. Suter, *All in the Family: Privacy and DNA Familial Searching*, 23 HARV. J.L. & TECH. 309 (2010).

9 *About Us*, 23ANDME, https://mediacenter.23andme.com/company/about-us/ (last visited Apr. 1, 2020); *Company Overview*, ANCESTRY, https://www.ancestry.com/corporate/about-ancestry/company-facts (last visited Apr. 1, 2020).

10 Ruth Padawer, *Sigrid Johnson Was Black. A DNA Test Said She Wasn't*, N.Y. TIMES (Nov. 19, 2018), https://www.nytimes.com/2018/11/19/magazine/dna-test-black-family.html?action=click&module=Editors%20Picks&pgtype=Homepage (describing the size of DNA companies).

11 Salvador Hernandez, *One of the Biggest At-Home DNA Testing Companies is Working With the FBI*, BUZZFEED NEWS (Jan. 31, 2019), https://www.buzzfeednews.com/article/salvadorhernandez/family-tree-dna-fbi-investigative-genealogy-privacy?utm_term=.bwr4RbeLnw#.bwr4RbeLnw (reporting that FamilyTree has opened up its database to the FBI).

unbridled genetic surveillance and a call to Congress to enact uniform regulations across federal, state, and local databases.[12]

I. WHAT IS DNA AND HOW DOES LAW ENFORCEMENT USE IT?

To properly understand the developments in DNA identification and the distinction between individual and familial searches it is necessary to have an understanding of the scientific and institutional framework that exists in the United States.

A. The Science of DNA Identification

Deoxyribonucleic acid, or DNA, is the building block of human genetic code and can be found in every human cell.[13] DNA is made up of four chemical bases: adenine, cytosine, guanine, and thymine, which are assembled into the iconic double helix structure.[14] Each cell contains twenty-three pairs of chromosomes, which are long chains of DNA bases (nucleotides), half of which are passed down from each parent to their child.[15] For our purposes, there are two types of relevant DNA; mitochondrial and nuclear.[16]

Mitochondrial DNA is a specific type of DNA that contains one small circular chromosome and is found in the mitochondria, the powerhouse of the cell.[17] Mitochondrial DNA makes up less than 1% of one's total DNA, but is unique in that it is passed down solely from the mother.[18] While mitochondrial searches are not as specific or accurate as the more common nuclear DNA search method, the technique allows for a broader reach as each maternal relative will have the exact same sequence.[19] This means that while it generally does not have the reliability required for criminal trials, it can be helpful for police investigations.[20] Mitochondrial DNA is also much more suitable for crime scene investigations where the DNA has partially degraded

---

12 Kreag, *supra* note 4, at 1498.

13 *See* Kaye, *supra* note 3, at 114 (explaining the structure of DNA).

14 *See* Elizabeth Stewart Tanaka, *Can You Protect Your DNA When Your Family Does Not? An Analysis of Familial DNA Usage in Criminal Investigations*, 12 QUINNIPIAC HEALTH L.J. 115, 118 (2008) (explaining the science behind DNA structure).

15 *Id.* at 118.

16 *Id.* at 118.

17 Philip Siekevitz, *Powerhouse of the Cell*, 197 SCI. AM. 131 (1957), https://www.jstor.org/stable/24940890?seq=1#metadata_info_tab_contents (detailing the purpose of mitochondria).

18 Tanaka, *supra* note 14, at 120.

19 *Id.* at 121.

20 *Id.* at 121.

because mass amounts of copies of mitochondrial DNA exist in each cell. In contrast, with nuclear DNA, a scientist would need to find another intact cell in order to string together a missing sequence.[21] However, mitochondrial DNA searches are mostly still a developing science for which the full potential remains to be realized.[22]

Nuclear DNA makes up the majority of one's DNA and is what is primarily used by law enforcement. Within nuclear DNA, about 2-3% contains genes or coding DNA.[23] This is how one might get their mother's eyes or their father's Huntington's disease. The other 98% of the DNA was long thought to serve no functional purpose and was thus popularly termed "junk" DNA, although more recent studies have shown that much of it has roles in regulating how the coding regions are used.[24] This "junk" DNA is what is primarily used for identification.[25] In total, each person has about three billion chemical base pairs that, in a string, form sequences to create genes.[26] The order of the chemical bases (A, C, G, T) in nuclear DNA is mostly the same from individual to individual, but some locations contain difference sequences.[27] The sequence difference at a specific location is referred to as an allele.[28] The variations and patterns in the sequences, or polymorphisms, create the ability to uniquely identify individuals.[29] The most popular type of polymorphism for DNA identification purposes is the short-tandem repeat, or STR, named for the several short patterns of repeated chemical base pairs in a row. STRs vary widely in length and copy number among people; thus, if enough STRs are looked at, each person will have a unique set of specific STRs.

The FBI standard, used in the federal database, CODIS, compares sequences at thirteen locations (loci), using a total of twenty-six alleles for the search.[30] A comparison of two DNA samples' alleles' STR patterns at those

---

21 *Id.* at 122–23 ("Degraded evidence is more likely to contain mtDNA capable of being sequenced partly because of the hundreds to thousands of copies of mtDNA in each cell as opposed to the two copies of nucDNA. The sheer volume of mtDNA in each cell increases the likelihood of finding DNA that is suitable for analysis in otherwise compromised evidence.").

22 *Id.* at 121.

23 Julie Agueros, *Liberty, Justice, and Technology: Why Familial DNA Searches Must Confront the Rigor of the American Political Process*, 48 No. 4 CRIM. L. BULLETIN Art. 6 (2012).

24 *Id.* at 6.

25 *Id.* at 6.

26 Tanaka, *supra* note14, at 118.

27 Kaye, *supra* note 3, at 115.

28 *Id.* at 115.

29 *Id.* at 115.

30 *Id.* at 119.

loci can determine whether the DNA comes from the same source.[31] Exact, complete matches between the crime scene DNA and the suspect's DNA mean that it is overwhelmingly likely that the suspect's DNA was present at the crime scene.[32] Similarly, anything but an exact match clears that suspect's DNA from the crime scene sample.[33] However, a close match, deemed a partial match, indicates that the suspect might share a genetic kinship with the crime scene DNA. The closer the match, the higher the probability that the two samples are related.[34]

There are three types of relevant matches: First, full matches, where the database profile contains every allele from the crime scene DNA, thus making the profile a suspect.[35] Second, partial matches, where the database profile contains alleles not found in the crime scene DNA, due to a variety of reasons such as a muddled sample, making the profile and its genetic relatives suspects. Third, familial matches, where the DNA profile differs from the crime scene sample in a way that clears the database inhabitant from suspicion, but makes it very probable that the inhabitant has a relative outside the database who was the source.[36] For now, due to the number of alleles tested, the familial match DNA analysis is only effective for close relations; parent-child, or full sibling relationships.[37]

With respect to the potential power of familial searches, a 1996 study reported that half of all inmates surveyed said they had close family members who had been incarcerated.[38] This is probably an underestimate of the technique's potential reach considering there are inmates' relatives who committed crimes and were not convicted as well as people's tendency to underreport bad behavior.[39] While it's impossible to measure the technique's efficacy in the real world, as the databases grow, both due to more people committing crimes and more actions being deemed worthy of DNA collection (recall the power creep of sex crimes to felonies, to crimes, to arrestees), its

---

31 *Id.* at 116.

32 *Id.* at 116.

33 *Id.* at 116.

34 *Id.* at 116. This is different from "the closer the match, the more closely the two DNA samples are related." While this might be true, it is not what DNA identification is testing for.

35 *Id.* at 121.

36 *Id.* at 121.

37 *Id.* at 120.

38 *Id.* at 123.

39 Nicole J. Olynk Widmar et al., *Social Desirability Bias in Reporting of Holiday Season Healthfulness*, PREVENTATIVE MED. REPORTS, Dec. 2016, at 270–76, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4942737/ (finding that social desirability bias causes people to underreport bad behavior, even in the benign context of holiday health habits).

range will only broaden.[40] Similarly, as the science behind DNA analysis improves and databases begin adding more alleles to the profiles, the technique itself will become more refined and more powerful.[41]

B. CODIS, the Federal DNA Database

CODIS, the Combined DNA Index System, is the federal database for DNA profiles. It was created in 1990 by the FBI[42] with the purpose of tracking sex offenders, but has since expanded drastically.[43] It is available to any approved law enforcement agency and has resulted in a massive number of hits and leads in cases.[44] As of March 2018, there are more than fourteen million known individuals in the database, and it has survived all legal challenges.[45] The CODIS database links all federal, state, and local databases.[46] It has two sections, the Forensic Index, which contains crime scene samples, and the Offender Index, which contains DNA from individuals compelled to provide genetic samples.[47] When CODIS was enacted, it was accompanied by a number of regulations regarding quality of the DNA sample, privacy concerns, and protocols regarding the expungement of profiles.[48]

The federal database is restricted by a regulatory framework enacted to protect privacy and shield it from legal challenges.[49] Such regulations include regular audits, a prohibition on familial searches, limited comparison abilities with partial matches, the removal of a DNA profile if the case is overturned or the arrestee dismissed, and the removal of consensual DNA samples, which are typically given by victims or suspects.[50] Additionally, the national labs can take up to a month to confirm a match and twelve months to create a profile.[51] These regulations limit the efficacy of the federal database, leading some

---

40 Kaye, *supra* note 3, at 123.

41 *Id.* at 124.

42 *See* Amanda Pattock, Note, *It's All Relative: Familial DNA Testing and the Fourth Amendment*, 12 MINN. J. L. SCI. & TECH. 851, 856 (2011) (noting the creation of CODIS).

43 Suter, *supra* note 8, at 317.

44 Pattock, *supra* note 42, at 858.

45 Kreag, *supra* note 4, at 1494.

46 Suter, *supra* note 8, at 316.

47 *Id.* The DNA Identification Act of 1994 carves out "DNA samples that are voluntarily submitted solely for elimination purposes" from being stored in the Index. 42 U.S.C. § 14132 (2006). However, "samples voluntarily contributed from relatives of missing persons" are permitted to be stored. *See* Suter, *supra* note 8, at 315.

48 Pattock, *supra* note 42, at 857.

49 Kreag, *supra* note 4, at 1502.

50 *Id.*

51 *Id.*

commentators to criticize it as ineffective, arguing that because it mostly contains violent offenders' DNA who are already in prison, it is redundant.[52]

C. Local Databases

State and local databases are not limited by these restrictions. The regulations on these databases are determined by the state legislature or in some cases, the self-regulation of the law enforcement agency.[53] This is problematic as law enforcement success is commonly measured by crime rates and clearance rates, so there is little incentive for the police to limit their investigative abilities.[54]

The first local database was started in Palm Bay, Florida, after a private DNA company approached the local police department in 2006.[55] Within six months, the database contained 1400 profiles, burglary rates had decreased, and clearance rates had increased.[56] The success of Palm Bay led to the spread of local databases, and by 2013, the other police departments in Florida had created their own databases and merged them with Palm Bay's database, creating a database of 13,000 profiles within a year.[57]

Local databases are typically characterized by aggressive collection of crime scene DNA.[58] This is typified by the index splits; the federal database is made up of about 94% offender profiles and 6% crime scene samples.[59] In contrast, the database for Bensalem, Pennsylvania has about a 50/50 split between forensic and offender data.[60] What this indicates is a focus on DNA searches for less serious crimes.[61] At the state level there are typically less restrictions on the databases than the federal system. For instance, one of the reasons Arizona developed its own state database was specifically for familial searches,[62] and Alabama and Michigan have authorized the retention and collection of DNA samples for medical research.[63] Notably in contrast,

---

52 *Id.* at 1503.

53 *Id.*

54 *Id.* at 1498.

55 *Id.* at 1507.

56 *Id.* at 1509.

57 *Id.* at 1510.

58 *See, e.g.*, *id.* at 1513 (describing the collection practices of the Bensalem, Pennsylvania township where DNA collection from suspects is typical).

59 *Id.* at 1512.

60 *Id.*

61 *See, e.g.*, *id.* (describing increased efforts to collect DNA in conjunction with property crimes).

62 *Id.* at 1532–33.

63 Suter, *supra* note 8, at 335.

Vermont banned non-federal databases and Maryland and Washington D.C. have banned familial searches.[64] However, most states in fact do not have formal regulations and policies, leaving local law enforcement agencies to decide their approach and defend it in court.[65]

Moving forward, DNA identification techniques are only going to become faster and more powerful.[66] Recent advances in testing have allowed scientists to gain more information from less DNA, both in terms of damaged samples and from new sources such as skin cells or saliva.[67] Tests are becoming faster and cheaper, and federal funding is increasingly going to local databases.[68] Finally, just as the Palm Bay local DNA database was jumpstarted by a corporate pitch, more companies are seeing law enforcement as a revenue stream and expanding their DNA testing and databanks.[69]

II. THE CONSTITUTIONALITY OF FAMILIAL DNA SEARCHES

A. The Constitutionality of DNA Databases and Searches

From their inception, DNA banks have been challenged in court, typically under the Fourth Amendment.[70] However they have survived all legal challenges, even as they expanded in reach and power.[71] Courts typically balance the intrusiveness and personal nature of DNA against a totality-of-the-circumstances, "reasonableness" of the search and the special needs of law enforcement to identify suspects and lower recidivism.[72]

---

64 MD. CODE ANN., PUB. SAFETY § 2-506(d) (LexisNexis 2020); D.C. Code Ann. §218.2(b) (West 2001).

65 Suter, *supra* note 8, at 336–37.

66 *See* Heather Murphy, *Coming Soon to a Police Station Near You: The DNA 'Magic Box'*, N.Y. TIMES (Jan. 21, 2019), https://www.nytimes.com/2019/01/21/science/dna-crime-gene-technology.html?action=click&module=Top%20Stories&pgtype=Homepage (commenting on the development of Magic Box, a new DNA technology).

67 Kreag, *supra* note 4, at 1504.

68 *Id.* at 1504–05.

69 *Id.* at 1506.

70 DNA evidence has never been held to be self-incrimination and worthy of Fifth Amendment protections. *See* United States v. Schmerber, 384 U.S. 757, 765 (1966) (finding that physical evidence such as blood is not testimonial or communicative in nature and as such is not protected by the right against self-incrimination). However, the extraction of bodily materials is a search and, therefore, must be considered reasonable in order to be constitutional. *Id.* at 767–68.

71 Osagie K. Obasogie, *The Dangers of Growing DNA Databases*, L.A. TIMES (Apr. 9, 2010), https://www.latimes.com/archives/la-xpm-2010-apr-09-la-oe-obasogie9-2010apr09-story.html (noting that 18 states had enacted legislation permitting the collection of DNA from arrestees); Kaye, *supra* note 3, at 130.

72 Suter, *supra* note 8, at 329–30.

The Fourth Amendment requires that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause . . . ."[73] Courts have interpreted the role of this amendment to protect privacy and regulate police action. All Fourth Amendment analyses must begin with the threshold question of what constitutes a search or seizure, because if the conduct in question is not a search or seizure, then the protections of the Fourth Amendment do not apply.[74] The examination typically proceeds either as a reasonable expectation of privacy or a property analysis. In *Katz,* the Court laid out the first of these paths, holding that what a person knowingly exposes to the public is not subject to Fourth Amendment protection.[75] However, what that person seeks to preserve as private may be constitutionally protected if the person had a subjective belief of privacy in that area and society is willing the recognize that belief as reasonable.[76] The other method of recognizing a search is through a property analysis, typified by Justice Scalia's majority opinion in *Jardines*, which held that police trespass onto the accused's tangible property was an unreasonable search and therefore a Fourth Amendment violation.[77]

Once a court has determined that a warrantless search and seizure has occurred, it must determine whether the search was either reasonable or in violation of the Fourth Amendment. Illustrative of this fault line with respect to DNA searches is *Maryland v. King*.[78] In 2008, the Maryland legislature authorized the expansion of its database by allowing the police to conduct a cheek swab of any suspect charged with a violent crime.[79] There were some protections if the suspect was ultimately not convicted, but the trigger for the sample collection was an arrest.[80] The defendant, King, was swabbed and matched to an unsolved break-in and rape, prompting the legal challenge.[81] King argued that the swab was inarguably a search and unconstitutional as it was looking for evidence of a different crime without any reasonable

---

73 U.S. CONST. amend. IV.

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

75 *Id.* at 351.

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

77 Florida. v. Jardines, 569 U.S. 1, 11 (2013).

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

79 *Id.* at 443.

80 *Id.* at 441.

81 *Id.*

individualized suspicion, distinguishable from a search incident to arrest.[82] However, the Supreme Court upheld the Maryland statute using a reasonableness analysis that balanced the defendant's privacy concerns with the government's interest in law enforcement.[83] While Court agreed that the swab was a search, it was minimally intrusive and arrested persons had a lowered expectation of privacy.

Additionally, the Court held that the primary purpose of the DNA search was identification, which was a special need beyond pure law enforcement, as it had implications for bail and the suspect's threat to the officers.[84]

Justice Scalia wrote a scathing dissent, pointing out the various problems with the majority's special needs rationale, notably that identification took far too long to be practical for the threat or bail arguments.[85] However, even assuming that Scalia was right, and that the majority's rationale is significantly weakened, *King* demonstrates that the utility of DNA had such a powerful effect on the Court that it was willing to be flexible with the requirements of the Fourth Amendment.

This primary purpose argument is known as the "special needs" exception. When the government has "special needs" beyond the typical law enforcement context, and is investigating for purposes other than law enforcement, situations can be balanced to uphold non-probable cause searches, sometimes without individualized suspicion, even if what they do results in criminal liability. One powerful special need that courts have found for DNA databases beyond identification[86] and reducing recidivism[87] is closure for victims. In *United States v. Kincaid,* the Ninth Circuit held that "by contributing to the solution of past crimes, DNA profiling of qualified federal offenders helps bring closure to countless victims of crime who long have languished in the knowledge that perpetrators remain at large." Upholding

---

82 Brief for Respondent at 21, Maryland v. King, 569 U.S. 435 (2013) (No. 12-207) (2013) ("so too has [the State] failed to establish any level of individualized suspicion that would have justified the search of respondent").

83 King, 569 U.S. at 448.

84 *Id.* at 453.

85 *Id.* at 471–72 (Scalia, J., dissenting) ("The truth, known to Maryland and increasingly to the reader: this search had nothing to do with establishing King's identity.").

86 *See* Illinois v. Lidster, 540 U.S. 419 (2004) (finding that a police checkpoint conducting suspicionless searches in response to a hit-and-run was primarily information-seeking and not a violation of the Fourth Amendment).

87 *See* Ewing v. California, 538 U.S. 11, 29 (2003) ("Ewing's sentence is justified by the State's public-safety interest in . . . deterring recidivist felons.").

the use of DNA profiling, the Ninth Circuit concluded that "together, the weight of these interests is monumental."[88]

B. The Spread of Familial DNA Searches

Recall that a standard DNA test compares the chemical base sequences at thirteen loci of crime scene DNA to a database inhabitant's profile and that a perfect match will have identical sequences at those thirteen loci.[89] If no perfect matches are found, law enforcement can order what is known as a familial search. The FBI defines a familial search as a "second deliberate search [of a DNA database] in order to identify close biological relatives of the perpetrator in the known offender database," which is only to be used after a failed initial match.[90] In this case, the offender database is searched not for a perfect thirteen-loci match, but for a partial match such as an eight-loci match, which would suggest a close biological relative.[91] This two-step process for a familial match removes about 99% of non-related DNA profiles.[92] The FBI's definition has been criticized though, as partial matches are sometimes found (and then used) inadvertently, rendering the "deliberate search" definition too narrow.[93] Additionally, familial searches have been maligned as they are functionally searches based on genetic association rather than due to individualized suspicion or a conviction.[94] Not all uses of familial DNA searches are controversial however. The technique has been used in instances of child support, missing persons cases, and even for the confirmation that Osama Bin Landen was the man the Navy SEALS killed.[95]

Just as England kickstarted the DNA identification movement in the 1980s that eventually made its way over to the United States, in 2003, England was the first county to formally authorize familial searches.[96] England's diminished notion of privacy has placed it at the forefront of the power creep that has characterized the movement.[97] England was the first country to allow for the

---

88 United States v. Kincade, 379 F.3d 813, 839 (9th Cir. 2004).

89 Suter, *supra* note 8, at 319.

90 *Id.* at 324.

91 *Id.* at 319–20.

92 Agueros, *supra* note 23.

93 Suter, *supra* note 8, at 324.

94 *Id.* at 358.

95 Kaye, *supra* note 3, at 113–14.

96 Suter, *supra* note 8, at 324.

97 *See* Frederick Bieber & David Lazer, *Guilt by Association*, NEW SCIENTIST, Oct. 23, 2004, at 20 (noting that the U.K. "became the first country to permit the DNA profile of anyone arrested to be kept indefinitely, regardless of whether they are subsequently convicted").

retention of arrestee DNA samples, regardless of subsequent conviction, and the familial search technique there is both widespread and uncontroversial.[98] The technique has found success in England, getting credited for solving at least nine cases by 2005.[99] By 2006, the technique gained limited acceptance in the U.S., with the FBI permitting CODIS familial searches as a last resort.[100] At the local level, some regions are conducting familial searches in an informal manner, leading one study to declare a "startling lack of transparency in rulemaking."[101] However, other jurisdictions have demonstrated apprehension towards the constitutional and privacy concerns concerning familial searching, waiting for express directive from their legislatures before engaging in the practice.[102]

The expansion of DNA search power and the allure of familial searches cannot be denied.[103] Due to the correlation between poverty, neighborhoods, and crime (not to mention any psychological factors), there is a high instance of crime running in a family, with "one study show[ing] that thirty percent of inmates had brothers who were also incarcerated, and another that 'nearly half of jail inmates had at least one close relative who had been incarcerated.'"[104] Familial searches could effectively double or triple the size of the DNA database and allow for police to use volunteered DNA from a suspect's family if the suspect refuses to provide a sample and they cannot get a court order.[105]

Additionally, familial searches have been used to revive cold cases[106] and exonerate long-imprisoned people.[107] For instance, police caught the prolific "Bind, Torture, Kill" serial killer, Dennis Rader, by analyzing DNA submitted by his daughter.[108] The technique was also famously used to catch the "Grim Sleeper," a Los Angeles-based serial killer who committed his murders over the course of thirty years.[109] In this case, the police partially matched DNA

---

98 *See* Duncan Carling, Note, *Less Privacy Please, We're British: Investigating Crime with DNA in the U.K. and the U.S.*, 31 HASTINGS INT'L & COMP. L. REV. 487, 495 (2008) (noting that arrestee sampling is "an accepted and widespread practice in the U.K.").

99 Suter, *supra* note 8, at 324–25.

100 *Id.* at 325–26.

101 *Id.* at 326.

102 *Id.*

103 *See id.* at 318 n.51 ("President Obama has even recently called for arrestees to have their DNA collected and stored in the national database.").

104 Suter, *supra* note 8, at 321.

105 *Id.* at 320–21.

106 Pattock, *supra* note 42, at 852.

107 Lina Hogan, Note, *Fourth Amendment - Guilt by Relation: If Your Brother is Convicted of a Crime, You Too May Do Time,* 30 W. NEW ENG. L. REV. 543, 549–50 (2008).

108 Suter, *supra* note 8, at 320.

109 Pattock, *supra* note 42, at 851–52.

found on a victim to Christopher Franklin, who was caught on a weapons charge a year prior.[110] Since Franklin was born after the first of the Grim Sleeper's killings, detectives investigated his more appropriately-aged family members, eventually using DNA collected from a thrown out pizza to find a perfect match with Franklin's father, solving the cold case.[111] And just as traditional DNA searching has exonerated an estimated 212 people, familial searching freed Darryl Hunt after an eighteen-year imprisonment when the brother of the true killer turned up in a CODIS search.[112] Surely, as familial searching and DNA databases become more powerful, these stories will become the norm rather than the newsworthy.

C. The Constitutionality of Familial DNA Searches

Despite the highlighted successes of familial DNA searches, it is understandable why the technique has caused some law enforcement agencies to wait for express authorization. As Justice Breyer wrote, "DNA identification may raise privacy concerns. Suppose a check of a convict DNA database reveals a near miss, thereby implicating a relative who has no record of conviction and was consequently not included in the bank. What kind of legal rules should apply?"[113] No court has tested the technique thus far, but commentators have pointed to the policy implications, Fourth Amendment, and Fourteenth Amendment as potentially raising issues.[114]

Consider a case where police retrieve DNA from a crime scene, run it through the offender database, and do not find a match. Next, they conduct a second query, a familial search (search A), which leads to a partial match to a person who has been incarcerated for ten years and thus could not have committed the crime. Then, the officers investigate the family members of the partial match, just as they did with the Grim Sleeper, and attempt to compel them into giving a DNA sample (search B). Could the DNA be compelled without individualized probable cause?

---

110 *Id.* at 152.

111 *Id.* at 852. Courts have held that a person has no privacy interest in their discarded DNA as it has been abandoned. *See* California v. Greenwood, 486 U.S. 35, 37 (1988) (holding that a person had no privacy interest in their trash); *see also* Commonwealth v. Cabral, 866 N.E.2d 429, 431 (Mass. App. Ct. 2007) (holding that police scrapping spit off a sidewalk was not a Fourth Amendment violation).

112 Hogan, *supra* note 107, at 549, 552.

113 Jeffrey Rosen, *Genetic Surveillance for All*, SLATE (Mar. 17, 2009), https://slate.com/news-and-politics/2009/03/genetic-surveillance-for-all.html (discussing Justice Breyer's foreword in a book on justice and technology).

114 Kaye, *supra* note 3, at 112, 125, 129.

Framing familial searches through a reasonableness test like that of *Maryland v. King* leads to a much closer balancing test.[115] Familial searches are distinct from the traditional DNA search because the people who the search is targeted at are not in custody; they have no diminished expectation of privacy, nor is there an interest in preventing their recidivism. Plainly, they suffer increased police scrutiny based on their relatives' past involvement with the criminal justice system.[116] Regarding search A, we are considering the database inhabitant's interest in not having his DNA be used to track his family.[117] While finding standing could be an issue (in the absence of compulsion of DNA), the information revealed during these investigations could lead to significant embarrassment and emotional injury in instances where genetic relations differ from social relations, notably in cases of adoption, adultery, incest, or assisted pregnancy.[118] This information could come to light inadvertently, or police could use it as leverage to pressure a person into revealing information.[119]

Additionally, the "special needs" rationale relied on by the *King* Court is significantly weakened in this instance. Familial searches serve purely law enforcement purposes, there is no threat to the officers nor any bail considerations to take into account. While the practice might have a broader social purpose, and as courts have noted, could provide a potential familial deterrent effect,[120] this is unlikely to fulfil the special needs requirement.[121] In *Ferguson v. City of Charleston*, the Supreme Court held that a hospital's policy of giving diagnostic medical records to a forensic lab served no special purpose. The Court reasoned that "[b]ecause law enforcement involvement always serves some broader social purpose or objective, under respondents' view, virtually any nonconsensual suspicionless search could be immunized under the special needs doctrine by defining the search solely in terms of its ultimate, rather than immediate, purpose."[122] Similarly here, the secondary query and DNA collection serves no special interest beyond aiding the law

---

115 *See* Hogan, *supra* note 107, at 580 (discussing balancing test that utilizes reasonableness and totality of the circumstances framework).

116 Suter, *supra* note 8, at 349.

117 The family members would not have a claim because they have no privacy interest in another individual's DNA.

118 Suter, *supra* note 8, at 343.

119 *Id.* at 345.

120 Once the practice becomes societally known, people will be aware that they are more likely to be caught if someone in their family has been arrested.

121 Pattock, *supra* note 42, at 868.

122 Ferguson v. City of Charleston, 532 U.S. 67, 84 (2001).

enforcement investigation, and therefore its permissibility must rely purely on a reasonableness balancing test.

Balancing societal interests against an individual's Fourth Amendment rights will likely result in the permissibility of familial searches. *Maryland v. King* and subsequent cases have shown just how favored DNA searches and databases are with respect to a balancing test.[123] If a court must balance the reasonableness of the search against its intrusive nature, then when taking into account the aforementioned successes in cold cases and exonerations, the societal interest will likely win out.[124] With respect to the "family secrets" argument, there would need to be a showing that familial searching is somehow more damaging and more likely to reveal information than other legal police investigatory methods.[125] Due to the success stories, the exonerations, and the legal precedents, a court is likely to find that under the totality of the circumstances, familial searching is not unreasonable.[126]

With respect to search B, in order for the police to use a partial match to compel production of DNA from family members, courts will require a warrant, and it is unclear whether the partial match alone will satisfy the probable cause standard. The collection of the DNA is undeniably a search, and the Court has shown an interest in protecting bodily integrity.[127] This is doubly true when the information gleaned has the potential to contain valuable and compromising private medical facts.[128] However, familial searches rely on the same "junk" DNA STR search that traditional DNA searches rely on,[129] meaning that they are unlikely to trigger the additional privacy protections that a court might provide for medical secrets.[130] Once again, there are no special needs when it comes to compelling DNA from family members not under arrest and no apparent exigency exists. Therefore, if the police attempt to compel DNA production from an

---

123 *See* Maryland. v. King, 569 U.S. 435, 460 (2013) (holding that DNA searches are akin to fingerprint identification).

124 *See* Pattock, *supra* note 42, at 864 (referencing Supreme Court cases where societal interest won out over individual privacy in cases of mandatory DNA collection and retention).

125 Kaye, *supra* note 3, at 145.

126 In United States v. Pool, 621 F.3d 1213, 1221 (9th Cir. 2010), *vacated as moot,* 659 F.3d 761 (9th Cir. 2011) the 9th Circuit seemed to indicate it was unconcerned with any constitutional issues stemming from this aspect of DNA retention ("It is questionable whether the person ... whose familial comparison helped focus the inquiry, has suffered any invasion of his or her constitutional right to privacy.").

127 Schmerber v. California, 384 U.S. 757 (1966).

128 *See* Skinner v. Ry. Labor Exec.'s Ass'n, 489 U.S. 602, 617 (1989) (noting how chemical analysis of urine can reveal facts about whether a person is epileptic, pregnant, or diabetic).

129 *See infra* Part III.B ("The FBI defines a familial search as a 'second deliberate search of a DNA database.'").

130 *Supra* Part II.B.

individual solely on the basis of a partial match, a court should require a warrant to be issued and must determine whether a partial match is sufficient to support a probable cause standard. This determination is likely dependent on the reliability of the query and the likelihood that the family member is the perpetrator.[131]

Finally, familial searches could be challenged under a Fourteenth Amendment equal protection claim. It's fairly clear that familial searches will have a disparate impact on certain communities, both racial and religious.[132] 28.5% of African-American men, 16% of Hispanic men, and 4.4% of white men will be convicted of a felony at some point during their life.[133] The disparate impact from these numbers will be additionally exacerbated by racially disparate arrest rates, which will also potentially place arrestees' DNA in a database. Their DNA will be added to a database that was not intended for familial searches when it was created, subjecting the arrestees and their families to lifelong genetic surveillance. Additionally, certain groups like Mormons, Hispanics, and low-income people tend to have larger families "and are therefore will be more vulnerable familial searches."[134] However, this disparate impact is unlikely to be enough to trigger strict scrutiny, and the law enforcement interests are surely sufficient to justify a rational basis.

The case that would generally control this issue is *Washington v. Davis*.[135] In that case, black applicants were rejected from becoming police officers because they failed a written test.[136] The unsuccessful black applicants brought a class action suit and won at the appellate level, with the court finding that the test had a racially disparate impact and was insufficiently related to job performance.[137] However, this ruling was reversed at the Supreme Court, with Justice White writing that there must be proof of discriminatory intent or purpose in order to invalidate a government statute.[138] A government action does not violate the Equal Protection Clause merely because it has a "racially

---

131 *See* Illinois v. Gates, 462 U.S. 213, 239 (1983) (explaining that in order for a magistrate to issue a search warrant, he must evaluate the evidence under a "flexible, common-sense," totality-of-the-circumstances approach. He must determine whether there is sufficient information to establish probable cause and his actions must be beyond a mere ratification of others' conclusions).

132 Kaye, *supra* note 3, at 128–29.

133 Agueros, *supra* note 23.

134 Kaye, *supra* note 3, at 127.

135 Washington v. Davis, 426 U.S. 229 (1976).

136 *Id.* at 232.

137 *Id.* at 236.

138 *Id.* at 246–48.

disproportionate impact."[139] This ruling was largely grounded in practical logic:

> A rule that a statute designed to serve neutral ends is nevertheless invalid, absent compelling justification, if in practice it benefits or burdens one race more than another would be far-reaching and would raise serious questions about, and perhaps invalidate, a whole range of tax, welfare, public service, regulatory, and licensing statutes that may be more burdensome to the poor and the average black than to more affluent white[s].[140]

Washington v. Davis created an intent requirement in order to trigger strict scrutiny on a facially neutral government action. The intent standard was further clarified in *Personnel Administrator of Massachusetts v. Feeney*, wherein the Supreme Court ruled that there was no equal protection violation even when a neutral law had a disproportionately adverse effect on a minority so long as the law was not passed with a discriminatory intent.[141] To be constitutionally improper, the legislature must have passed the law "because of" the disparate impact, not "in spite of" it.[142]

Applying that framework to familial DNA searches, it is clear that there is no Fourteenth Amendment violation. While some protected groups are disproportionally affected, this is a facially neutral apparatus with no racial animus.[143] It will not trigger struct scrutiny, and the increased legitimacy and accuracy of DNA identification will survive a rational basis test.

III. THE FACTUAL AND LEGAL FRAMEWORK OF COMMERCIAL DNA DATABASES

A. The Science Behind Commercial Databases

In 2007, 23andMe became the first company in the world to offer commercial DNA testing.[144] By 2011, the company had 100,000 customers and in 2020 it reported that it had over ten million.[145] It is not alone; Ancestry, launched in 2012, has over sixteen million DNA profiles in its databank as of

---

139 *Id.* at 239.

140 *Id.* at 248.

141 Pers. Adm'r of Mass. v. Feeney, 442 U.S. 256, 272 (1979).

142 *Id.*

143 *See* Kaye, *supra* note 3, at 128 (arguing that discrimination and equal protection claims against the practice of familial searches would be "implausible.").

144 *About Us*, 23ANDME, https://mediacenter.23andme.com/company/about-us/ (last visited Mar. 13, 2019).

145 *23andMe History*, 23andMe, https://mediacenter.23andme.com/assets/timeline/index.html (last visited Apr. 1, 2020); *About Us*, 23ANDME, https://mediacenter.23andme.com/company/about-us/ (last visited Apr. 1, 2020).

April 2020.[146] To use the companies' products, customers submit their saliva for DNA analysis and the companies use the DNA to create individualized family trees, conduct medical research, and reveal medical facts about the customer's genetic profile. The companies are open to everyone and actively seek out underrepresented groups,[147] but by their expensive and (arguably) impractical nature have skewed towards a wealthier, whiter clientele.[148]

The companies seem to be aware of their attractive nature to law enforcement, with 23andMe noting that "about 80 percent [of surveyed Americans] said they had privacy concerns around DNA testing, much of that concern stems from not knowing how their data would be protected," and that 17 percent said privacy concerns stopped them from purchasing a test.[149] Some companies, such as Family Tree DNA, already are working with law enforcement, allowing FBI agents to search their database.[150] The big two companies, Ancestry and 23andMe, however, offer a defense of customers' genetic privacy even in the face of law enforcement requests.

Ancestry has a privacy page and releases a transparency report every year.[151] Its privacy page notes that it will "share your Personal Information if [Ancestry] believe[s] it is reasonably necessary to comply with [a] valid legal process (e.g., subpoenas [or] warrants)."[152] Further, the company says that while a user can request to have their information deleted, if they have consented to help with research, the data cannot be deleted.[153] In 2017, Ancestry's transparency report stated that it received thirty-four requests from law enforcement for user information; however, all of the requests were related to financial transactions and none asked for genetic material.[154] That said, Ancestry has supplied

---

146 *Company Overview*, ANCESTRY, https://www.ancestry.com/corporate/about-ancestry/company-facts (last visited Apr. 1, 2020).

147 *The African Genetics Project*, 23ANDME: 23ANDMEBLOG (Oct. 12, 2016) https://blog.23andme.com/23andme-research/the-african-genetics-project/.

148 Isabelle Mencia, *Why DNA Ancestry Tests are Struggling to Avoid White Bias*, STUDY BREAK (Mar. 5, 2018) https://studybreaks.com/news-politics/dna-ancestry-tests/.

149 *National Survey Shows Strong Interest in DNA Testing*, 23ANDME (Sept. 18, 2017) https://mediacenter.23andme.com/press-releases/national-survey-shows-strong-interest-dna-testing/.

150 Hernandez, *supra* note 11.

151 *Privacy Statement Archive*, ANCESTRY, https://www.ancestry.com/cs/legal/privacy-archive (last visited Apr. 1, 2020).

152 *Website Privacy Statement*, ANCESTRY, https://www.ancestry.ca/cs/legal/privacystatement (last visited Mar. 12, 2019).

153 *Id.*

154 *Ancestry 2017 Transparency Report*, ANCESTRY, (Dec. 31, 2017) https://www.ancestry.ca/cs/transparency.

genetic information to law enforcement in the past, notably in 2014, which led to a false-positive match.[155]

23andMe's privacy page claims to be "technically and legally" secure from law enforcement, and boasts of having never given genetic info to them.[156] Allegedly, this is because they test for a different sequence (STP) rather than the STR pattern that CODIS uses.[157] Additionally, 23andMe claims that their service cannot be reliably connected to an individual in a verifiable manner such that it could be used in court.[158] To use 23andMe, a person orders a spit-kit and then mails their DNA sample to the company.[159] Because the person who ordered the kit and the one who gave the sample are not necessarily the same person, the company claims that the DNA cannot be validated as belonging to the named person.[160] While this does seem to be a surmountable issue, 23andMe maintains that they have never given information to a law enforcement agency.[161]

B. The Relevant Doctrines and Caselaw

Building off of the analysis that DNA tests are permissible under the Fourth Amendment and that familial DNA searches would survive both Fourth Amendment and Fourteenth Amendment challenges, police use of commercial DNA databases brings with it its own set of legal issues. Commercial database DNA involves personal information willingly given to a company for non-law-enforcement purposes. Additionally, the collected DNA contains not only "junk" DNA but also the "coding" DNA that contains the personal information needed to create a commercial genetic profile.[162]

---

155 Jennifer Lynch, *How Private DNA Data Led Idaho Cops on a Wild Goose Chase and Linked an Innocent Man to a 20-year-old Murder Case*, ELEC. FRONTIER FOUND. (May 1, 2015) https://www.eff.org/deeplinks/2015/05/how-private-dna-data-led-idaho-cops-wild-goose-chase-and-linked-innocent-man-20.

156 Kate Black & Zerina Curevac, *23andPrivacy: Your Data and Law Enforcement*, 23ANDME: 23ANDMEBLOG (Mar. 16, 2016), https://blog.23andme.com/23andme-and-you/23andprivacy-your-data-law-enforcement/.

157 *Id.*

158 *Id.*

159 *Id.*

160 Stephanie M. Lee, *Cops Want to Look At 23andMe Customers' DNA*, BUZZFEED NEWS (Oct. 21, 2015), https://www.buzzfeednews.com/article/stephaniemlee/law-enforcement-is-interested-in-23andme-user-data.

161 Black & Curevac, *supra* note 156.

162 DNA is composed of coding and non-coding regions. Non-coding DNA, termed "Junk" DNA is what is used to identify a person, but does not show more invasive characteristics like genetic traits. *See* King, 569 U.S. at 442–43. Coding DNA is what is used by commercial companies as it contains the genetic traits such as ancestry and illnesses.

Despite all this, police use of these databases should be permissible, at least constitutionally, due to the lack of a reasonable expectation of privacy once one has given away their non-essential records to a third-party.[163]

In *United States v. Miller*, police used the defendants' bank transactions as evidence that they were participating in a criminal conspiracy.[164] The defendants tried to suppress the transactions under the theory that they had a reasonable expectation of privacy in those documents and that it was improper for the police to seize the paperwork without a warrant.[165] The Supreme Court upheld the conviction, ruling that once someone has shared information with a third-party, they no longer have a reasonable expectation of privacy with respect to that information.[166] The Court additionally pointed to precedent supporting the notion that deposit slips are elements of commercial transactions and therefore unprotected.[167] Also pertinent is *United States v. White*, where the Court held that even misplaced expectations of trust (talking to an informant) are unprotected, despite the chilling effects it may have.[168] Thus, until recently, anything given to a third party, even if under a misplaced expectation of privacy, lacked constitutional protection.

The Supreme Court however has begun to narrow the third-party doctrine,[169] likely due to how much information is being sent to data companies. Described most succinctly in Justice Sotomayor's *Jones* concurrence, there is a concern that so much of daily life is indispensably and inadvertently being shared that the third-party doctrine threatens to completely erase the Fourth Amendment.[170] This issue notably arose in *United States v. Carpenter*, wherein the police used cell phone tracking technology to locate a defendant without a warrant.[171] In a 5-4 holding, the Court held that despite an individual "giving" his location through his cell phone to a third-party (the cell tower companies), he still had a reasonable expectation of privacy.[172] The Court recognized that expectations of privacy in the digital age produce new challenges that do not align with precedent, and that the personal "nature of

---

163 United States v. Miller, 425 U.S. 435, 443 (1976). The Court articulated the impact third parties have on one's reasonable expectation of privacy. However, *Miller* did not address the distinction between essential and non-essential records nor the permissibility of DNA searches.

164 *Id.* at 436.

165 *Id.* at 442.

166 *Id.* at 440.

167 *Id.* at 440–441.

168 United States v. White, 401 U.S. 745, 751–52 (1971).

169 Carpenter v. United States, 138 S.Ct. 2206 (2018); United States v. Jones, 565 U.S. 400 (2011).

170 Jones, 565 U.S. at 415–16.

171 Carpenter, 138 S.Ct. at 2212.

172 *Id.* at 2217.

the particular documents sought" carved out an exception to the third-party doctrine.[173] This holding was bolstered by the indispensable nature of cell phones and the lack of voluntary affirmative action on the individual's part.[174]

In a broad reading of *Carpenter's* holding, Professors Freiwald and Smith identified several factors that the Court used in defining its carve-out in addition to the classic *Katz* test: Whether the investigatory method was hidden, continuous in its tracking nature, indiscriminate in what information and how much information the police had access to, intrusive in revealing deeply personal information, and whether the expense of the search would allow law enforcement to obtain a tremendous amount of information that, if using more traditional techniques, would have taken much longer and cost much more to acquire.[175] Using these factors, the Court reined in the third-party doctrine, leaning on *Riley*[176] to show that the assumption of risk framework inherent in the third-party doctrine is not mechanical, but rather has some components of voluntary and knowledgeable action.[177] In the wake of *Carpenter*, Freiwald and Smith called for a "closer analysis when it comes to privately maintained databases of non-location information" as *Carpenter* "wipes out" the argument that information "merely by [its] storage with a third party, [is] immune from Fourth Amendment protection by virtue of the third-party doctrine."[178]

While *Carpenter* and *Jones* dealt with electronic tracking technology, there is other precedent that suggests the Court will not be willing to extend the third-party doctrine to information given for diagnostic purposes. In *Ferguson v. City of Charleston*, a hospital partnered with law enforcement to submit pregnant women's blood given for diagnostic reasons to a forensic lab in order to test for cocaine content.[179] The policy was designed to reduce cocaine usage among pregnant women, which was harming the unborn child, after previous attempts requiring mandatory therapy, education, and treatment were found ineffective.[180] The Court held that this was a violation of the Fourth Amendment despite the medical information being given to a third-party (the hospital) because of a patient's reasonable expectation that medical

---

173 *Id.* at 2217–18.

174 *Id.* at 2218.

175 Susan Freiwald & Stephen Wm. Smith, *The Carpenter Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 220–21 (2018) (emphasis added).

176 Riley v. California, 134 S.Ct. 2473, 2494 (2014) (giving special protection to cell phones due to their indispensable and personal nature).

177 Freiwald & Smith, *supra* note 175, at 224–25.

178 *Id.* at 230.

179 Ferguson, 532 U.S. at 69–70.

180 *Id.* at 70.

information would not be disseminated without her consent.[181] The Court further rejected any special needs exception noting the involvement of law enforcement at every step of the process, and the general interest in crime control.[182] While not expressly stated, the Court may have also been weighing the negative externality of disincentivizing cocaine-using women from giving birth at a hospital.

When considering the use of new technology for searches, it is also necessary to survive the *Kyllo* test. There, police used a thermal imager to scan a house in search of marijuana-growing glow lamps.[183] This technology was new at the time and was used without a warrant.[184] The Court suppressed the information gathered because "[w]here . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[185] While homes generally have enhanced privacy protection, the concept of regularly-used technology not triggering additional protections is potent in the present instance.

IV. ANALYSIS

On what grounds could law enforcement gain access to the wealth of data that Ancestry, 23andMe, and other similar companies possess? Do customers have any reasonable expectations of privacy in their information once given away? What about in the case of FamilyTree, which was both named the best company for "strict privacy"[186] and was the first to openly volunteer for FBI cooperation?

A. Police Use of Commercial DNA Banks Should be Constitutionally

---

181 *Id.* at 78.

182 *Id.* at 79–80; *see also* City of Indianapolis v. Edmond, 531 U.S. 32, 44 (2000) (internal citations omitted) ("The primary purpose of the Indianapolis narcotics checkpoints is in the end to advance 'the general interest in crime control.' We decline to suspend the usual requirement of individualized suspicion . . . . ").

183 Kyllo v. United States, 533 U.S. 27, 29 (2001).

184 *Id.* at 30, 40.

185 *Id.* at 40.

186 Brad Berman, *Best DNA Testing Kits*, U.S. NEWS & WORLD REPORT (Jan. 7, 2019), https://health.usnews.com/wellness/articles/2019-01-07/best-dna-testing-kits; Dieter Holger, *FamilyTreeDNA Review: Unique Genealogical Collaboration, But an Outdated Interface*, PCWORLD (Dec. 14, 2018, 5:00AM PST), https://www.pcworld.com/article/3326568/familytreedna-review.html.

Permissible

Following *Katz*, a court would need to find that someone, either the user or the company has an objectively reasonable expectation of privacy in the DNA in order to gain the protections of the Fourth Amendment. The court should hold that a user has no reasonable expectation of privacy in their DNA once it has been sent to a company, though with the recent narrowing of the third-party doctrine it is not completely obvious that the State has an overpowering interest. The court should also hold that an individual does not have a claim for constitutional protection under the *Kyllo* framework nor a property interest in their DNA. Further, the evidentiary defense that 23andMe raised seems solvable with circumstantial evidence authenticating the sample and the testimony of the scientist who did the testing in accordance with *Melendez-Diaz*.[187] However, the court should hold that the companies have a privacy interest, or at least that law enforcement will be required to conduct a pre-compliance review before a neutral party prior to accessing the genetic records.

The most persuasive argument for cutting back the third-party doctrine for commercial DNA banks is the "personal nature of the information." The DNA samples sent in contain private medical facts, something that could give them some protection, as in *Skinner*.[188] Applying the *Carpenter* factors identified by Freiwald and Smith leaves questions as to whether the third-party doctrine would even apply. Certainly, commercial DNA searches would be hidden, done in secret, away from the public view. The search would not be continuous but would be inarguably indiscriminate in the amount of people captured by the search (especially considering benign family members), and intrusive given the personal nature of genetic material. Finally, DNA testing is becoming increasingly cheap and quick, implicating the expense factor.[189] The court could also look to *Ferguson* to carve out a third-party exception. There, the Supreme Court found patients to have a reasonable expectation of privacy in information given for diagnostic purposes.[190] Similarly, many people undergo genetic testing in order to discover potential illnesses and submit their DNA for research purposes, which society should not disincentivize.[191] Finally, due to the privacy statements provided by the companies, the

---

187 Melendez-Diaz v. Mass., 557 U.S. 305, 311 (2009).

188 Skinner, 489 U.S. at 617.

189 Murphy, *supra* note 66.

190 Ferguson, 532 U.S. at 78.

191 23andMe, *supra* note 156.

individuals certainly have a subjective expectation of privacy that their information will not be disseminated.

The court should find however that the third-party doctrine does extend to commercial DNA banks. Inarguably, customers of these companies took an affirmative action in giving away their information to a third-party. The customers consented to the storage and use of the data, and their misplaced trust in a company that they were told was the best for "strict privacy" would be an inadequate argument under *White*.[192] Further cutting against the rationale of the *Carpenter* majority that carved out a modern-age exception to the third-party doctrine, there is nothing "essential" or "indispensable" about DNA tests. Cell phones are ubiquitous and necessary to modern life; they contain pictures, addresses, and are how we contact loved ones in emergencies. They even gain heightened protection compared almost any other object.[193] The court should not find that this is the case for DNA tests. Customers did not need to give their DNA to a company in the same way that a soon-to-be mother is vulnerable to a doctor's orders. In response to the "personal nature of the information" argument, if law enforcement only requested the information obtained from the "junk" DNA, then this argument is unlikely to be persuasive, as no private medical information will be disclosed. Additionally, the DNA sample could be thought of as an element of the commercial transaction and therefore, also receive no constitutional protection.[194] The court should also not recognize a *Kyllo* argument to find a reasonable expectation of privacy, because at this point the general public is using DNA testing.[195]

With respect to the property theory of the Fourth Amendment, it is similarly unlikely that a consumer could make a successful property claim on their DNA once it is given away.[196] In *Moore v. Regents of California,* a physician-scientist at UCLA took diagnostic samples of Moore's blood and bone marrow and unbeknownst to Moore, used them for research.[197] Moore's

---

192 *See* United States v. White, 401 U.S. 745, 749 (1971) (holding that misplaced trust doesn't create a reasonable expectation of privacy).

193 *See* Riley v. California, 134 S.Ct. 2473, 2494–95 (2014) (finding that absent exigent circumstances, police can seize the phone, but need a warrant to actually search the data inside).

194 Miller, 425 U.S. at 442.

195 Kyllo, 533 U.S. at 34.

196 For an argument that the Fourth Amendment does provide some protection of DNA property and that legislatures should enact policies regarding DNA testing websites, *see* Antony Barone Kolenc, *"23 and Plea": Limiting Police use of Genealogy Sites after Carpenter v. United States*, 122 W. VA. L. REV. 54, 100–01 (2019).

197 Moore v. Regents of Univ. of California, 793 P.2d 479, 481 (Cal. 1990).

cells turned out to be scientifically and commercially significant, leading to substantial profit and many discoveries, so Moore brought suit claiming he had a property right to his cells.[198] The Supreme Court of California found that Moore had no property rights to his discarded cells or to the research or profits made from the cell lines. The court rejected the argument that someone has an absolute right to the unique products of their body.[199]

The commercial DNA companies here are using the DNA for research and commercial purposes. Further, the informed consent here is being done in much more comprehensive ways than in *Moore*. While customers can request their DNA profiles to be deleted, this is not true if the profiles are being used for research, which is the case for many of the profiles. A court is unlikely to find that customers have any property interest in their abandoned DNA.

One issue to note is the potential mitigation of Fourteenth Amendment claims with the proliferation of police use of commercial DNA databases. Due to the underrepresentation of African-American and Native American samples in the commercial databases, police currently actually have a much more powerful database for investigating wealthier, white suspects. While this would not alleviate the concerns against religious groups, the continued lack of discriminatory intent would ultimately defeat any such claim.

With respect to 23andMe's chain-of-custody argument, this appears to be a solvable problem with good police and prosecutorial work. Matching the user (who sent in the sample) to the buyer (who purchased the sample) could be confirmed through witness interviews, or at least provide a lead through the purchaser who might know the user. With respect to testimony in court, the initial DNA sample was not analyzed in preparation for use at a judicial proceeding, so it is unlikely to be held to be testimonial and therefore trigger the Sixth Amendment Confrontation Clause.[200] Even if it were analyzed for such a purpose, 23andMe stated that it has had five requests by law enforcement since 2007. It would not be an intolerable burden for a scientist (or the law enforcement forensic scientist who ran the CODIS match) to testify to the procedure's accuracy.[201] Commercial DNA database users are unlikely to have any constitutional protections in their submitted samples. The data was freely and affirmatively given, and their misplaced trust does not protect

---

198 *Id.* at 487.

199 *Id.* at 489, 491.

200 Melendez-Diaz, 557 U.S at 310.

201 *See* Bullcoming v. New Mexico, 564 U.S. 647, 683–84 (2011) (Kennedy, J., dissenting) (citing the burdens on forensic scientists as a reason for his dissent).

them. Nor will the users' families have any constitutional protections involving the user's DNA for the same reasons mentioned above in the familial search analysis.[202]

Finally, there are the privacy rights of the companies themselves to consider. Given the economic power that comes from the privacy and security of genetic data, it is clear that the companies have an interest in keeping that information secure.[203] The case most analogous to this situation is *City of Los Angeles v. Patel*, in which the Los Angeles Code required hotels to retain the information of their guests for up to 90 days.[204] If the hotel failed to do so or failed to turn over the records to the police upon request, the owner faced criminal penalties.[205] The Supreme Court struck down this policy, holding it an unreasonable search and seizure.[206] It held that in order to conduct a warrantless search of a hotel, there must be some sort of pre-compliance review before a neutral party.[207] While the Court recognized the hotel's interest in its records, it did not expressly recognize that the hotel had a reasonable expectation of privacy. Rather, this case turned on whether the hotel industry fell under the administrative search "special needs" exception by being a "closely-regulated industry."[208] A closely-regulated industry is one that presents a clear and significant risk to public welfare such as firearms, mining, or running an automobile junkyard.[209] DNA companies do not fall into this category, and as such will be able to require some pre-compliance review before any information is provided. As Ancestry and 23andMe both note that they require subpoenas or a warrant before they turn over any information, it is likely that they would support this argument.[210]

---

202 *See supra* note 126 and accompanying text.

203 City of L.A. v. Patel, 135 S.Ct. 2243, 2248 (2015), *quoting* Patel v. City of Los Angeles, 738 F.3d 1058, 1065 (9th Cir. 2013) ("[t]he business records covered by § 41.49 are the hotel's private property" and the hotel therefore "has the right to exclude others from prying into the[ir] contents.").

204 *Id.* at 2447–48.

205 *Id.* at 2448.

206 *Id.* at 2452.

207 *Id.*

208 *Id.* at 2454.

209 *Id.*

210 Privacy Pages, *supra* note 152, 152.

CONCLUSION

Familial DNA searching is still new, but we have seen numerous examples of damaging false positives, including from commercial DNA banks.[211] Beyond just DNA searches, the bungled 2006 Duke Lacrosse investigation[212] and the Reddit witch-hunt[213] in the aftermath of the Boston Marathon Bombings illustrate the destructive cloud of suspicion that mishandled investigations can cause. Even if the investigation is handled correctly, an unknown family link, or lack thereof could damage a family in a way that is not legally cognizable. Yet the positives surely outweigh the danger. Murderers have been caught, innocent people have been exonerated, and the DNA searching technology will only become more accurate. Familial DNA searching, even using commercial databanks, is not a practice that should be done away with.

Since there is unlikely to be constitutional protection given to the users or their family members, and only limited protection given to companies, it is up to the legislatures to enact regulations and protections at all levels of government. While the state of genetic surveillance in the U.S. is nowhere near the nightmare that is China,[214] the lack of regulations at the local level has led to increased surveillance of innocent people.[215] Local databases "are

---

[211] Erin E. Murphy, *Familial DNA* Searches, 27 CRIM. JUST. 19 (2012) (arguing against police use of familial DNA searches given the ethical and legal concerns they raise). *See also* Jim Mustian, *New Orleans Filmmaker Cleared in Cold-case Murder; False Positive Highlights Limitations of Familial DNA Searching*, THE N. ORLEANS ADVOCATE (Mar. 12, 2015) available at https://www.theadvocate.com/new_orleans/news/article_1b3a3f96-d574-59e0-9c6a-c3c7c0d2f166.html (documenting how a familial DNA search caused an innocent filmmaker to become a suspect in a murder investigation); *Federal DNA Collection*, ELEC. FRONTIER FOUND., https://www.eff.org/cases/federal-dna-collection (last visited Mar. 13, 2019) (underscoring the privacy concerns involved in federal DNA collection policies); Lynch, *supra* note 155.

[212] *See* Zach Schonbrun, *Ex-Duke Lacrosse Coach Rebuilds Shattered Career*, N.Y. TIMES, (May 16, 2014) available at https://www.nytimes.com/2014/05/17/sports/ex-duke-lacrosse-coach-rebuilds-shattered-career.html?rref=collection%2Ftimestopic%2FDuke%20Lacrosse%20Sexual%20Assault%20Case&action=click&contentCollection=timestopics&region=stream&module=stream_unit&version=latest&contentPlacement=5&pgtype=collection. (detailing the impact and aftermath of one woman's false sexual assault allegations against three Duke University lacrosse players).

[213] Alyson Shontell, *What It's Like When Reddit Wrongly Accuses Your Loved One of Murder*, BUS. INSIDER, (July 26, 2013) available at https://www.businessinsider.com/reddit-falsely-accuses-sunil-tripathi-of-boston-bombing-2013-7.

[214] Sui-Lee Wee, *China Uses DNA to Track Its People, With the Help of American Expertise*, N.Y. TIMES, (Feb. 21, 2019) available at https://www.nytimes.com/2019/02/21/business/china-xinjiang-uighur-dna-thermo-fisher.html?action=click&module=Top%20Stories&pgtype=Homepage (describing China's use of American DNA technology to oppress Uighur racial minorities through coercive and surreptitious gathering of DNA).

[215] Kreag, *supra* note 4, at 1529.

designed with the assumption that they will ultimately include a large number of DNA profiles from people who will never be linked to a crime."[216]

Moving forward, legislatures should adopt the European approach, where law enforcement cannot use an investigative method until it has been authorized by statute.[217] At the minimum, there should be a uniform set of regulations in order to minimize silver-plattering.[218] Legislatures must rise to the challenge. They must enact regulations to provide better notice to those who volunteer their data for non-law enforcement purposes and to protect those who right now are protected only by the evolving whims of a company's internal policies.

---

[216] *Id.* at 1530.

[217] Freiwald & Smith *supra* note 175, at 235 (citing Kiel Brennan-Marquez & Stephen E. Henderson, *Fourth Amendment Anxiety*, 55 AM. CRIM. L. REV. 1, 33 (2018) (footnote omitted) ("[W]hen privacy and liberty norms are in flux, as they currently are given recent and rapid technological change, police *should* seek the assistance of legislatures in governing investigatory methods, and they *must* seek the approval of courts."); Susan Freiwald & Sylvain Métille, *Reforming Surveillance Law: The Swiss Model*, 28 BERKELEY TECH. L.J. 1261 (2013) (discussing the advantages of a Swiss surveillance law over reforms proposed in the United States)).

[218] Where law enforcement duties get shuttled to the level with the most discretion.