All in the Family: A Fourth Amendment Analysis of Familial Searching

Lindsey Weiss, University of Chicago
All in the Family: A Fourth Amendment Analysis of Familial Searching
Lindsey Weiss

I. INTRODUCTION ..................................................................................................................2
II. DNA DATABANKS AND FAMILIAL SEARCHING: HISTORY, SCIENCE, EXAMPLES, AND EXPANSION ..........................................................4
   A. Federal DNA Databases .................................................................................................4
   B. The Scientific Basis of DNA Identification .................................................................5
   C. Examples of Successful Familial Searching .................................................................6
   D. Recent Database Expansion .........................................................................................7
III. THE FOURTH AMENDMENT .........................................................................................8
IV. CURRENT DNA INDEXING CASE LAW .......................................................................10
   A. The Special-Needs Test .................................................................................................10
   B. The General Balancing Test .......................................................................................12
V. EXISTENCE OF A FOURTH AMENDMENT SEARCH OF CONVICTED PERSONS’ FAMILY MEMBERS ..........................................................................................................12
   A. Sources of Privacy .........................................................................................................14
      1. Genetic privacy ...........................................................................................................14
      2. Family privacy ...........................................................................................................15
         a. Favish: Informational family privacy .....................................................................15
         b. Favish: Analysis and application ..........................................................................16
         c. Borough of Barrington: Informational family privacy .......................................18
         d. Borough of Barrington: Analysis and application .............................................18
   B. Familial Searching as a Fourth Amendment Search ...............................................19
      1. Subsequent use ...........................................................................................................21
      2. Role of technology ....................................................................................................22
      3. Voluntariness ............................................................................................................23
      4. Control .....................................................................................................................25
      5. Unfit analogies ...........................................................................................................25
         a. Family resemblance ..............................................................................................26
         b. Fingerprinting .........................................................................................................26
VI. THE SPECIAL-NEEDS TEST .......................................................................................27
   A. Familial Searching: Existence of a Special Need ....................................................27
VII. FAMILIAL SEARCHING AS A CONSTITUTIONALLY UNREASONABLE USE ........................................................................................................28
VIII. CONCLUSION .............................................................................................................30
I. INTRODUCTION

Over the past twenty years, the use of DNA databanks for law enforcement purposes has grown exponentially. In 1989, Virginia became the first state to establish a database that contained DNA from convicted criminals.\(^1\) In 1991, Minnesota became the first state to solve a “cold case” using a DNA database match.\(^2\) Today, all states maintain DNA databases of known offenders, though different states operate their systems according to different guidelines.\(^3\) These state systems are connected to a national system known as the Combined DNA Information System (CODIS) that is run by the FBI.\(^4\)

In recent years, law enforcement officials have learned to identify partial DNA matches that present a high likelihood that the DNA left at the crime scene belongs to a family member of the known offender. This technique, known as familial searching, has been used to close at least fifteen cases in the United Kingdom\(^5\) and has also been used in the disposition of several cases in the United States.\(^6\)

Circuit courts have unanimously upheld the constitutionality of DNA databases against Fourth Amendment challenges brought by convicted persons, based largely on convicted felons’ diminished expectation of privacy.\(^7\) No court, however, has addressed a Fourth Amendment challenge to familial searching based on the privacy interests of convicts’ family members, who have not forfeited their privacy rights.

Former FBI policy prohibited states from sharing names with one another in the event of a partial match.\(^8\) In July 2005, Thomas Callaghan, director of the FBI database program, claimed that, “Federal privacy law bars the FBI from performing familial searches within its own database.”\(^9\) In July 2007, however, the FBI instituted an interim policy that allows states to decide whether to share information with one another based on partial matches.\(^10\)

---

1. Henry F. Fradella, From Legal Literature, 43 No 4 Crim Law Bulletin 7 (July–August 2007).
2. Id.
3. See id.
7. See, for example, United States v Kincade, 379 F3d 813 (9th Cir 2004).
8. See Finkelstein, A Not So Perfect Match at 1 (cited in note 6).
10. Finkelstein, A Not So Perfect Match at 3 (cited in note 6). See also Willing, DNA Near Matches Spur Privacy Fight, USA Today at 3A (cited in note 5).
The new FBI policy took very little time to spur controversy. In August of 2007, California Attorney General Edmond Brown refused to release the name of a near-match to Denver District Attorney Mitchell Morrissey, an advocate of familial searching. Brown cited the need to protect the privacy of the California felon, and claimed that familial searching overreached current case law authorizing DNA databanks. Other states, including Oregon and Arizona, have shared information based on near-matches with Morrissey. In April of 2008, Brown did an about-face, when he announced that California, whose database holds more than one million people, would be the first state to rigorously use familial searching as a matter of policy.

In light of the FBI’s current policy and the growing popularity of familial searching among states, analysis of the privacy issues raised by familial searching can help illuminate responsible public policy, legislation and judicial decisions regarding familial searching. Both Callaghan’s and Brown’s statements express an intuition that something about familial searching seems troubling. Many involved in the legal field share a similar intuition that subjecting “a whole new class of innocent people to genetic surveillance by the government” raises significant privacy issues. Some argue that if familial searching is permitted, convicted persons essentially forfeit not only their own privacy rights, but also those of wholly innocent family members.

Generally, little has been written about familial searching. In the summer of 2006, the Journal of Law, Medicine and Ethics published a symposium titled “DNA Fingerprinting and Civil Liberties.” Several articles in the symposium touched on the history, science, ethics or potential effects of familial searching. All the articles, however, either failed to address, or swiftly dismissed, a potential Fourth Amendment challenge to familial searching.

This Comment will explore whether familial searching constitutes a violation of convicted persons’ family members’ constitutional rights. First, it will analyze whether familial searching represents a Fourth Amendment search of convicted persons’ family members. After analyzing the possibility of a Fourth Amendment search, this Comment will evaluate whether such a search could be considered constitutionally reasonable based on the special-needs test. Additionally,

---

11 Willing, DNA Near Matches Spur Privacy Fight, USA Today at 3A (cited in note 5).
12 Id.
13 Id.
15 Finkelstein, A Not So Perfect Match at 1 (cited in note 6).
16 See id.
17 See generally, Alice A. Noble, DNA Fingerprinting and Civil Liberties, 34 JL Med & Ethics 149 (Summer 2006).
18 See id at 150.
19 See, for example, Greely, 34 JL Med & Ethics at 257 (cited in note 9) (dismissing Fourth Amendment concerns on the grounds that relatives of known offenders have been neither searched nor seized, and concluding that family privacy cases do not apply).
this Comment will consider whether the systematic practice of familial searching constitutes a constitutionally unreasonable use of legally collected convict DNA, and thus could invalidate DNA indexing laws as long as familial searching persists.

In Part II, this Comment will provide information about important background issues related to familial searching. It will discuss the history and current state of DNA databases, the scientific basis for familial searching, notable examples of familial searching, and recent expansion of DNA databases.

In Part III, this Comment will provide a brief overview of Fourth Amendment law, highlighting important issues, themes, and lines of cases that are central to analyzing a potential Fourth Amendment challenge to familial searching.

In Part IV, this Comment will discuss current case law regarding DNA databanks. It will discuss the current circuit split over the appropriate test to apply when analyzing the constitutionality of DNA indexing statutes, and will summarize both the “special-needs” and “general balancing” tests.

In Part V, this Comment will analyze whether familial searching represents a Fourth Amendment search of convicts’ family members. This Part will begin by examining how currently recognized privacy interests support finding individuals have a reasonable expectation of privacy in their family members’ DNA. Based on these privacy interests, it will demonstrate that familial searching should constitute a Fourth Amendment search of convicted persons’ family members.

In Part VI, this Comment will explore whether familial searching could be justified based on the special-needs test.

In Part VII, this Comment will discuss whether familial searching constitutes a constitutionally unreasonable use of otherwise lawfully collected convict DNA.

II. DNA DATABANKS AND FAMILIAL SEARCHING: HISTORY, SCIENCE, EXAMPLES, AND RECENT EXPANSION

A. Federal DNA Databases

The federal DNA database, called the National DNA Index System (NDIS), comprises two different indexes as part of the CODIS.\(^\text{20}\) The “Forensic Index” contains profiles from crime scene evidence.\(^\text{21}\) The “Offender Index” contains the profiles of individuals convicted or charged with crimes submitted by state or federal law enforcement groups.\(^\text{22}\) Law enforcement agencies can check DNA profiles against either of these indexes to connect a convicted person to a recent crime, a suspected person to a past crime, or to link current and past crimes.

\(^{20}\) Id at 250–51.  
\(^{21}\) Id at 251.  
\(^{22}\) Id.
As of June 2008, NDIS contained over six million convicted offender profiles, and over two hundred thousand forensic profiles.\textsuperscript{23} In recent years, the number of DNA profiles contained in the NDIS has rapidly expanded by more than one million profiles per year (containing 2,599,959 convicted offender samples in 2005, 3,977,433 in 2006, 5,070,434 in 2007, and 6,031,000 as of June 2008).\textsuperscript{24} According to the FBI, CODIS has aided more than 71,800 criminal investigations.\textsuperscript{25}

B. The Scientific Basis of DNA Identification

The average adult is comprised of between 50 and 100 trillion cells.\textsuperscript{26} Nearly every cell contains a nucleus with 46 chromosomes made of deoxyribonucleic acid (DNA).\textsuperscript{27} Nested within the vast majority of our DNA that has no known function (known as “junk DNA”\textsuperscript{28}) are different stretches of sequence called “short tandem repeats” (“STRs”) that can be used for identification.\textsuperscript{29}

In the United States, crime laboratories use sets (or pairs) of 13 STRs spread over 12 chromosomes (providing 26 total alleles) for genetic identification purposes.\textsuperscript{30} The odds that two unrelated people share the same set of 13 pairs is at most one in several hundred billion.\textsuperscript{31} Identical twins will share all 26 alleles, and first-degree relatives (parents, siblings, children) will share at least half.\textsuperscript{32} By contrast, two random Americans on average will share only two or three alleles.\textsuperscript{33} This much higher rate of commonality among relatives facilitates familial searching.

Typically, searches of the CODIS database look for perfect matches, and the lack of such a match is considered a failure.\textsuperscript{34} But a partial match can indicate, to a high degree of probability, that the crime scene DNA came from someone closely related to the known offender.\textsuperscript{35} For instance, parent/child matches are distinct because they must match at no fewer than 13 alleles,

\textsuperscript{24} Id.
\textsuperscript{25} Id. But see Rothstein and Talbott, 34 JL Med & Ethics at 154 (cited in note 4) (arguing that although “these totals make for good headlines and legislative testimony . . . their use raises a number of serious methodological and policy concerns”).
\textsuperscript{26} Greely, 34 JL Med & Ethics at 249 (cited in note 9).
\textsuperscript{27} Id.
\textsuperscript{28} These STRs were selected because they are not associated with known physical or medical characteristics. Kincade, 379 F3d at 818. However, some studies have questioned “the notion that junk DNA does not contain useful genetic programming material.” Id at n 6.
\textsuperscript{29} Greely, 34 JL Med & Ethics at 249–50 (cited in note 9).
\textsuperscript{30} Id at 250. These are also known as “CODIS markers.”
\textsuperscript{31} Id.
\textsuperscript{32} Id.
\textsuperscript{33} Id.
\textsuperscript{34} Id at 251.
\textsuperscript{35} Id.
because one of the child’s two alleles at each of the 13 pairs came from the parent. This unusual pattern (they must match at one allele at each marker) allows scientists to identify not only a high probability of relation, but also the probable nature of the relation. The chance that two unrelated people will produce a match that mimics a parent/child relationship, however, is about one in two thousand. Although these odds are low, with over six million people in the NDIS, an average profile is likely to produce several thousand spurious matches.

Due to the existence of spurious matches, usually a partial match is not overwhelming evidence of relation, but merely a lead. The strength of that lead is likely to depend on whether the DNA profile is common or rare, and how strong or weak the lead is can be estimated. The likelihood law enforcement will choose to follow-up on partial-match leads often depends on the number of matches, type of crime, and the existence of alternative leads.

To increase the efficiency of familial searching, CODIS could increase the number of genetic markers (or pairs) analyzed for DNA identification. Adding even 20 additional markers would greatly increase the probability of identifying familial ties, and would almost entirely eliminate spurious leads. Because law enforcement agencies could potentially increase the number of genetic markers, and thus identify family relationships with near accuracy, this Comment will analyze the constitutionality of familial searching assuming a high probability of certainty.

C. Examples of Successful Familial Searching

One of the most publicized examples of successful familial searching occurred in England in 2003. Just after midnight on March 21, 2003, Michael Little’s truck was hit by a brick

36 Id at 252.
37 Id. Similarly, siblings share not only a high number of overall matching markers (about 16.7 on average), but also a pattern of matching alleles that indicates a sibling relationship. Id at 253.
38 Id. (These odds vary depending on ethnicity. Id at n 22).
39 See id.
40 Id.
41 Id at 254.
42 Id.
43 The current number of CODIS markers were chosen in order to give a high degree of certainty for exact matches, before law enforcement organizations realized the potential of low-stringency analysis (familial searching). As more and more law enforcement agencies attempt to harness familial searching’s potential, it is likely there will be a greater push to increase the number of genetic markers. One potential barrier to increasing the accuracy of familial searching, however, will be staffing and funding constraints. Even under the current system, large DNA backlogs prompted the federal government to pass legislation to fund states’ efforts to reduce the backlog of more than 500,000 samples. Crime Lab’s Massive DNA Backlog. CBS News, Apr 6, 2004, online at http://www.cbsnews.com/stories/2004/04/06/tech/main610514.shtml (visited Aug 27, 2008).
44 Fradella, 43 No 4 Crim Law Bulletin 7 (cited in note 1).
thrown off an overpass as he drove down a highway. The brick crashed through the truck’s windshield and hit Little in the chest, triggering a fatal heart attack. Although the police had no suspects, the brick thrown from the overpass contained blood from both the victim and another source, presumably the perpetrator. The DNA on the brick did not match any profiles in the British DNA database, and voluntary DNA samples taken from over 350 men in the area provided no leads.

After little success in the investigation, British police decided to check the DNA database for partial matches. After narrowing partial matches to include only young white males from the area, the police interviewed the person with the closest match and discovered he had a brother living near the scene of the crime. The brother, Craig Harmon, at first denied involvement, but volunteered a DNA sample. His DNA matched that found on the brick, and after being confronted with this evidence, he confessed.

Familial searching is less common in the United States compared to the United Kingdom. The most publicized United States’ case was featured on CBS news in July of 2007. In North Carolina, police used familial searching to solve a brutal rape and murder that had been committed 23 years earlier. In that case familial searching not only allowed police to find an otherwise untraceable perpetrator, but also exonerated an innocent man who had been convicted of the crime and had already served 19 years in prison.

D. Recent Database Expansion

Until recently, those included in CODIS were largely limited to persons convicted of committing a limited number of traditionally violent felonies. On January 5, 2006, President Bush signed into law a federal statute that authorizes the collection of DNA samples from

---

45 Greely, 34 JL Med & Ethics at 248 (cited in note 9).
46 Id.
47 Id.
48 Id.
49 Id.
50 Id.
51 Id.
52 Id.
53 See id.
54 See generally Finkelstein, A Not So Perfect Match (cited in note 6).
55 Id at 3.
56 Id. Although DNA evidence had already exonerated the person convicted of the crime, he was not released until familial searching revealed the true perpetrator. Id.
57 See, for example, DNA Analysis Backlog Act of 2000, Pub L No 106-546, § 3, 114 Stat 2726, 2728 (codified as amended at 42 USC § 14135a) (providing for DNA collection for individuals convicted of murder, manslaughter, sexual abuse, child abuse, kidnapping, robbery, burglary or any attempt or conspiracy to commit such crimes).
individuals arrested or detained by federal authority for inclusion in CODIS.\textsuperscript{58} Essentially, the Act empowers the Attorney General to collect samples from arrestees and detainees, but requires the Director of the FBI to expunge the samples of persons that are not subsequently convicted.\textsuperscript{59} Additionally, a majority of states allow some misdemeanors to qualify for inclusion in CODIS,\textsuperscript{60} and an increasing number of state laws permit the collection of DNA from mere arrestees.\textsuperscript{61} These samples collected by the states are included in CODIS.

The recent expansion of CODIS to include not only offenders convicted of violent crimes, but also those convicted of mere misdemeanors, and those arrested but not yet convicted or absolved, alters current case law regarding the validity of DNA indexing. As is explained in greater depth below, current case law that upholds DNA indexing relies on a convicted person’s diminished expectation of privacy.\textsuperscript{62} Although the recent expansion of CODIS may alter existing case law, the alteration may be limited by the fact that some cases suggest arrestees also have a diminished expectation of privacy.\textsuperscript{63}

III. THE FOURTH AMENDMENT

The Fourth Amendment states: “The 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. . .”\textsuperscript{64} When determining the existence of a search or seizure in early Fourth Amendment cases, courts focused on whether evidence was collected from a “constitutionally protected area.”\textsuperscript{65} However, in Katz v United States,\textsuperscript{66} the Supreme Court found that “the Fourth Amendment protects people, not places.”\textsuperscript{67} The Court found that the Fourth Amendment is not limited to protecting physical penetration of tangible property, but instead extends to protecting the privacy upon which an individual justifiably

\textsuperscript{59} Id.
\textsuperscript{62} See, for example, United States v Amerson, 483 F3d 73 (2d Cir 2007).
\textsuperscript{63} See Jones v Murray, 962 F2d 302, 307 (4th Cir 1992) (“[W]hen a suspect is arrested upon probable cause, his identification becomes a matter of legitimate state interest and he can hardly claim privacy in it.”).
\textsuperscript{64} US Const Amend IV.
\textsuperscript{65} See, for example, Weeks v United States, 232 US 383 (1914); Hester v United States, 265 US 57 (1924); Silverman v United States, 365 US 505, 510 (1960).
\textsuperscript{66} 389 US 347 (1967).
\textsuperscript{67} 389 US at 351.
relied. Justice Harlan’s concurrence provided the new test for determining a Fourth Amendment search: “[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and second, that the expectation be ‘one that society is prepared to recognize as reasonable.’” In practice, the second requirement (that the individual had a reasonable expectation of privacy in the evidence collected) has become determinative.

Because the Fourth Amendment protects against only unreasonable searches and seizures, after determining that a Fourth Amendment search has occurred, courts must assess the reasonableness of that search. Typically, this reasonableness requirement mandates that law enforcement officials have both a warrant and probable cause to undertake a search or seizure. Where neither a warrant nor probable cause exists, searches usually must be based upon some level of individualized suspicion.

The Supreme Court, however, has found that warrantless, suspicionless searches may be justified “when special needs, beyond the normal need for law enforcement, make the warrant and probable cause requirement impracticable.” Examples of proper special-needs searches include “searches conducted at the border, in prisons, at airports . . . student and employee drug tests; information-seeking checkpoints; and searches of probationers’ residences.”

When the subject of a warrantless, suspicionless search is a parolee or conditional releasee, the Supreme Court has held that courts may instead apply a general balancing test to determine the reasonableness of the search. Warrantless, suspicionless searches that fail both the special-needs and general balancing tests are deemed unconstitutional, and are subject to the Fourth Amendment’s general exclusionary rule.

---

68 389 US at 353 (finding that the “Government’s activities in electronically listening to and recording petitioner’s words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a ‘search and seizure’ within the meaning of the Fourth Amendment”).
69 Id at 361 (Harlan concurring).
70 Stephen E. Henderson, Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search, 56 Mercer L Rev 507, 517 (2005) (“Because the first requirement is often difficult to determine and is subject to government manipulation—for example a law enforcement announcement that all homes will hereafter be subject to random inspections—the second requirement has become determinative.”).
71 US Const Amend IV.
74 Amerson, 483 F3d at 80.
75 Nicolas, 430 F3d at 660-61 (footnotes omitted).
IV. CURRENT DNA INDEXING CASE LAW

Although the Supreme Court has never ruled on the validity of DNA indexing statutes under the Fourth Amendment, all seven federal circuit courts that have addressed Fourth Amendment challenges brought by convicted persons have found DNA indexing laws constitutional. In *Skinner v Railway Labor Executives Association*, the Supreme Court held that the “collection and subsequent analysis of [] biological samples must be deemed Fourth Amendment searches,” because they invade the defendants’ reasonable expectation of privacy. Accordingly, every court to consider the constitutionality of DNA indexing statutes has found that DNA indexing infringes upon convicted persons’ reasonable expectations of privacy, and therefore constitutes a Fourth Amendment search. Courts are divided, however, over the correct test to apply to evaluate the reasonableness these searches.

A. The Special-Needs Test

The Second, Seventh, and Tenth Circuits, along with a number of federal district and state courts, have adopted the special-needs test to evaluate the constitutionality of DNA indexing as a Fourth Amendment search. Using the two-prong special-needs approach, these courts examine: (1) “whether the search and seizure is justified by a special need beyond the ordinary needs of normal law enforcement,” and (2) “whether the search was reasonable in light of that special need.” These courts determine the reasonableness of the search by “weighing the government’s interest against the intrusion on the Appellants’ privacy interests.”

Courts have found that although “‘normal law-enforcement objectives’ cannot qualify as special needs, ‘some special law enforcement concerns’ will justify suspicionless searches under the special-needs doctrine.” These courts have found that “[a]lthough the state’s DNA testing of inmates is ultimately for a law enforcement goal, it falls within the special-needs analysis because ‘it is not undertaken for the investigation of a specific crime.’

---

78 *Green v Berge*, 354 F3d 675, 677 (7th Cir 2004).
79 See *Amerson*, 483 F3d at 78 n 3.
81 Id at 616.
82 See, for example *Kincade*, 379 F3d at 821; *Amerson*, 483 F3d at 77; *Green*, 354 F3d at 676; *United States v Kimler*, 335 F3d 1132, 1146 (10th Cir 2003).
83 *Kincade*, 379 F3d at 830; see also *Amerson*, 483 F3d at 78; *Green*, 354 F3d at 677–78; *Kimler*, 335 F3d at 1146.
84 *Amerson*, 483 F3d at 80.
85 Id.
86 Id.
87 Id at 81 (quoting *Nicolas*, 430 F3d at 663) (internal citations omitted).
88 *Green*, 354 F3d at 678.
89 Id.
In City of Indianapolis v Edmund,\textsuperscript{90} the city used motor vehicle checkpoints to interdict illegal narcotics trafficking. The Supreme Court distinguished the checkpoints from other permissible special-needs searches\textsuperscript{91} and found that the primary purpose of the checkpoint was to “detect evidence of ordinary criminal wrongdoing.”\textsuperscript{92} Because the checkpoints lacked a special need, the Court found they violated the Fourth Amendment.\textsuperscript{93} The Seventh Circuit attempted to distinguish Edmund from DNA indexing by finding that the primary purpose of DNA indexing is not to “search for evidence of criminal wrongdoing” but instead “to obtain reliable proof of a felon’s identity.”\textsuperscript{94}

After determining a special need exists, these courts judge the reasonableness of the search based on three factors: “(1) the nature of the privacy interest involved; (2) the character and degree of the governmental intrusion; and (3) the nature and immediacy of the government’s needs, and the efficacy of its policy in addressing those needs.”\textsuperscript{95} In executing this balancing test, the Second Circuit identified two distinct privacy interests DNA indexing statutes infringe upon: (1) the physical intrusion in extracting the DNA sample,\textsuperscript{96} and (2) the “analysis and maintenance of [offenders’] information.”\textsuperscript{97} The Second Circuit considered this second infringement a “potentially much more serious invasion of privacy” than the actual physical intrusion.\textsuperscript{98}

Despite the DNA indexing statutes’ infringement on these privacy rights, courts that use the special-needs test have found that the convicted person’s significantly reduced expectation of privacy, particularly in his or her identity, greatly reduces the infringement.\textsuperscript{99} After comparing this “quite small,”\textsuperscript{100} invasion of privacy against the government’s “strong, even compelling and monumental interest in obtaining and storing accurate identifying information from convicted offenders,”\textsuperscript{101} these courts have found DNA indexing statutes are reasonable, and thus constitutional.\textsuperscript{102}

\begin{itemize}
  \item[^{90}] 531 US 32 (2000).
  \item[^{91}] The Court distinguished the checkpoints in question from drunk-driving checkpoints, which aimed to remove drunk drivers from the road for safety purposes, and checkpoints designed to intercept illegal aliens, which served a border control function. 531 US at 37–38.
  \item[^{92}] 531 US at 42.
  \item[^{93}] 531 US at 48.
  \item[^{94}] Green, 354 F3d at 678.
  \item[^{95}] Cassidy v Chertoff, 471 F3d 67, 75 (2d Cir 2006).
  \item[^{96}] Amerson, 483 F3d at 84.
  \item[^{97}] Nicholas, 430 F3d at 670.
  \item[^{98}] Amerson, 483 F3d at 85. In determining the scope of this second infringement, the court in Amerson found “the DNA profile derived from the offender’s blood sample establishes only a record of the offender’s identity.” Id. It noted, however, if it were discovered that junk DNA could be used in significantly greater ways, “a reconsideration of the reasonableness balance struck would be necessary.” Id at n 13.
  \item[^{99}] See, for example, id at 85–86.
  \item[^{100}] Id at 87.
  \item[^{101}] Id.
  \item[^{102}] See, for example, id.
\end{itemize}
B. The General Balancing Test

Many courts have argued that the special-needs test does not apply to parolees and conditional releasees.103 In United States v Kincade,104 the Court recognized that “parolees and other conditional releasees are not entitled to the full panoply of rights and protections possessed by the general public,”105 and that restrictions placed on convicted persons “dramatically alter the relationship between the releasee and the government.”106 Based on this disrupted relationship, along with the government’s interest in monitoring persons previously convicted of crimes, the Court found that the existence of a “special need” was not necessary to justify a search “where such searches meet the Fourth Amendment touchstone of reasonableness as gauged by the totality of the circumstances.”107

The Third, Fourth, Fifth, Ninth, and Eleventh Circuits, as well as numerous federal district and state courts, have used this balancing test to evaluate DNA indexing statutes.108 In conducting the reasonableness test, these courts have found the convicted persons’ significantly diminished expectation of privacy, balanced with the overwhelming societal interests in sheltering society from future victimization, weighs in favor of allowing DNA indexing as a reasonable search under the Fourth Amendment.109

The courts that have adopted the “totality of the circumstances” test have largely failed to address whether a special need might exist.110 Thus, while three circuit courts have found DNA indexing constitutes a special need, the remaining circuits have abstained from considering the issue.

V. EXISTENCE OF A FOURTH AMENDMENT SEARCH OF CONVICTED PERSONS’ FAMILY MEMBERS

To date, no court has considered the constitutionality of familial searching. To successfully challenge familial searching, family members of convicted persons must be able to

---

103 The Supreme Court precedents that established and developed the special-needs test fail to condemn suspicionless searches of conditional releasees’ in the absence of a “special need.” Kincade, 379 F3d at 832.
104 Id at 813.
105 Id at 833.
106 Id at 834.
107 Id at 835.
108 See United States v Sczubelek, 402 F3d 175, 184 (3d Cir 2005); Jones, 962 F2d at 307; Groceman v DOJ, 354 F3d 411, 413 (5th Cir 2004); Kincade, 379 F3d at 832; Padgett v Donald, 401 F3d 1277, 1280 (11th Cir 2005).
109 See, for example, Kincade, 379 F3d at 839.
110 See, for example, Padgett, 401 F3d at 1278 n 4 (“Because we uphold the statute under a totality of the circumstances analysis, we do not address whether it could satisfy a ‘special needs’ analysis.”); Kincade, 379 F3d at 832 (emphasizing that by adopting the totality of the circumstances analysis, the court was “not precluding the possibility that the federal DNA Act could satisfy a special needs analysis”).
assert a reasonable expectation of privacy in convicted persons’ DNA. The Supreme Court has found that “Fourth Amendment rights are personal rights and may not be asserted vicariously.” 111 A “defendant’s Fourth Amendment rights are violated only when the challenged conduct invaded his legitimate expectation of privacy rather than that of a third party.” 112 Courts have found a reasonable expectation of privacy is one that has “a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.” 113

This Part V sets forth a potential Fourth Amendment challenge to familial searching. In Section A, this Comment analyzes sources of genetic and family privacy that support finding individuals have a reasonable expectation of privacy in their family members’ DNA. In Section B, this Comment argues that because of these privacy interests, familial searching constitutes a Fourth Amendment search of convicts’ family members.

A. Sources of Privacy

Although circuit courts have unanimously upheld the constitutionality of DNA databases against Fourth Amendment challenges raised by convicted persons, no court has addressed whether familial searching violates the privacy interests of convicts’ family members, who have not forfeited their privacy rights. To determine the constitutionality of familial searching, it is therefore necessary to explore the nature and extent of family members’ privacy interest in one another’s DNA.

Privacy law is notable in that judges and scholars commonly look to other areas of law in determining its scope. This has been true since its inception. Many view The Right to Privacy, 114 an 1890 article by Samuel Warren and Louis Brandeis, as the birth of privacy law. 115 In that article, Warren and Brandeis argue for the creation of a new right, the right to privacy, by drawing together principals gleaned from “legal analogies already developed in the law of slander and libel, and in the law of literary and artistic property.” 116

In many seminal privacy cases the Supreme Court has cobbled together a range of legal sources to support its decisions. For instance, the Court in Roe v Wade 117 discussed the various “roots” of the right to privacy found in the First, Fourth, Fifth, Ninth, and Fourteenth Amendments. 118 By drawing upon a number of these sources, the court determined that the right to privacy “is broad enough to encompass a woman’s decision whether or not to terminate her

115 For instance, Roscoe Pound has written that the article “did nothing less than add a chapter to our law.” Alpheus Mason, Brandeis: A Free Man’s Life 70 (The Viking Press 1946).
116 Warren and Brandeis, 4 Harv L Rev at 214 (cited in note 114).
117 410 US 113.
118 410 US at 153.
pregnancy.” Similarly, in determining the scope of family members’ privacy interest in one another’s DNA, this Comment will draw from a variety of legal sources.

Individuals have at least three potential types of privacy interests in their family members’ DNA. First, the collection of convicts’ DNA potentially violates family members’ privacy interest in their genetic information because the DNA of one individual provides vast amounts of genetic information about his or her immediate family members, including kinship, genetic predispositions, race characteristics and genetic defects. Second, familial searching potentially violates family members’ privacy interest in their genetic identity because the collection of DNA from one individual can subject his or her family members to lifelong genetic surveillance.119 Third, given the current inaccuracy of familial searching, its practice potentially violates family members’ privacy interest in being free from government investigation, absent suspicious or illegal conduct, because its practice greatly increases the probability that convicts’ family members will become suspects for crimes they did not commit.120

Support for these privacy interests can be drawn from sources of genetic and family privacy law. Analysis of these sources support finding individuals have a robust privacy interest in their genetic information, including their genetic identity, regardless of whether it is obtained from their own DNA, or from that of a family member.

1. Genetic privacy.

The majority of states have passed laws protecting an individual’s right to privacy in his or her genetic information.121 For instance,

Laws in 17 states require informed consent for a third party either to perform or require a genetic test or to obtain genetic information. Twenty-seven states require consent to disclose genetic information. Alaska, Colorado, Florida, Georgia, and Louisiana explicitly define genetic information as personal property. Alaska also extends personal property rights to DNA samples. . . . Four states mandate individual access to personal genetic information, and 19 states have established specific penalties - civil, criminal or both - for violating genetic privacy laws.122

119 Genetic identity is really just one type of genetic information. Thus, it should be considered included in the discussion of genetic information. This Comment will also consider this privacy infringement separately, however, because familial searching specifically exploits genetic identity, making it the most important kind of genetic information for the purpose of this Comment.
120 Although this privacy interest is potentially important, this Comment focuses on familial searching assuming a high probability of certainty. Therefore, this privacy interest is largely outside the scope of this Comment.
122 State Genetic Privacy Laws at 1 (cited in note 121).
These statutes recognize both a privacy interest and a property interest in genetic information. That a majority of state legislatures has found it necessary to guarantee the protection of genetic privacy indicates individuals have a robust privacy interest in their genetic information.

Courts have also recognized this strong privacy interest. As discussed, in Skinner the Supreme Court found the subsequent analysis of individuals’ biological samples violated their reasonable expectation of privacy.123 In United States v Amerson,124 the court noted that it was “mindful of the vast amount of sensitive information that can be mined from a person’s DNA and the very strong privacy interests that all individuals have in this information.”125

Similarly, in his concurring opinion in Kincade, Judge Gould observed:

[U]nlike fingerprints, DNA stores and reveals massive amounts of personal, private data about that individual, and the advance of science promises to make stored DNA only more revealing over time. Like DNA, a fingerprint identifies a person, but unlike DNA, a fingerprint says nothing about the person's health, their propensity for particular disease, their race and gender characteristics, and perhaps even their propensity for certain conduct.126

Viewed together, these sources suggest that individuals have a strong privacy interest in the vast amount of genetic information, including genetic identity, stored in their DNA. The following analysis of family case law explores whether this robust privacy interest in genetic information persists when that information is obtained not from one’s own DNA, but from that of a family member.

2. Family privacy.

Two notable family privacy cases, National Archives and Records Administration v Favish,127 and Doe v Borough of Barrington128 support the conclusion that family members have a robust privacy interest in one another’s DNA.

a) Favish: Informational family privacy. Current case law supports finding individuals can assert a privacy interest in information about their family members. In National Archives and Records Administration v Favish,129 Allen Favish filed suit to compel production of photographs taken by the United States Park Police at the death scene of Vincent Foster Jr., deputy counsel to President Clinton.130 Although the government concluded that Foster had

123 Id at 616.
124 483 F3d 73 (2d Cir 2007).
125 Id at 85.
126 379 F3d at 842 n 3 (Gould concurring).
130 Id at 160–61.
committed suicide, Favish remained skeptical, and filed a Freedom of Information Act (FOIA) request for pictures of Foster’s body at the scene of his death.\textsuperscript{131}

The government refused the request under Exemption 7(C) of the FOIA 5 USC § 552.\textsuperscript{132} The Court interpreted the exemption, which excuses disclosure of information collected for law enforcement purposes when it “could reasonably be expected to constitute an unwarranted invasion of personal privacy.”\textsuperscript{133} The Court held that the exemption’s protection against “an unwarranted invasion of personal privacy” extended to family members of the person police had investigated.\textsuperscript{134} The Court found the right to personal privacy “is not confined . . . to the right to control information about oneself.”\textsuperscript{135}

Justice Kennedy, writing for a unanimous majority, found, “There is special reason . . . to give protection to . . . intimate personal data, to which the public does not have a general right of access in the ordinary course.”\textsuperscript{136} Kennedy noted that Favish’s family members did not attempt to invoke the exemption on behalf of Foster, but rather were attempting to “invoke their own right and interest to personal privacy” in the information.\textsuperscript{137} Kennedy found that although the family was not “in the same position as the individual who is the subject of the disclosure,” they nonetheless possessed a personal privacy interest in the photographs.\textsuperscript{138}

\textit{b) Favish: Analysis and application.} Favish supports family privacy interests relevant to DNA indexing generally and familial searching specifically in four important ways. First, Favish held that family members have a privacy interest in information about one another. DNA contains vast amounts of information about the person from whom it is obtained. Favish supports finding that individuals have a privacy interest in their family members’ DNA because it contains information about their family members.

Second, Favish specifically dealt with information (photographs) collected by the government for law enforcement purposes. Favish, therefore, indicates that family members do not lose their privacy interest in information when the government legally obtains that information for law enforcement purposes. Convicts’ DNA (and consequently their genetic information) is collected under DNA indexing statutes for law enforcement purposes. Thus,

\begin{itemize}
  \item \textsuperscript{131} Id at 161.
  \item \textsuperscript{132} Id.
  \item \textsuperscript{133} § 522(b)(7)(C).
  \item \textsuperscript{134} 541 US at 170.
  \item \textsuperscript{135} Id at 165 (internal quotation marks omitted).
  \item \textsuperscript{136} Id at 166.
  \item \textsuperscript{137} Id.
  \item \textsuperscript{138} Id at 167. Courts have also recognized that family members have a personal privacy interest in information about their family members in other contexts. See Reid v Pierce County, 136 Wn 2d 195, 212 (1998) (“[T]he immediate relatives of a decedent have a protect able privacy interest in the autopsy records of the deceased”); McCambridge v Little Rock, 298 Ark 219, 231–32 (1989) (recognizing a mother’s privacy interest in crime scene photographs of her deceased daughter’s body).
\end{itemize}
Favish supports protecting individuals’ privacy interest in their family members’ genetic information even when legally collected under DNA indexing statutes.

Third, the Court found it was important to extend privacy protection to “intimate personal data, to which the public does not have a general right of access in the ordinary course.”\(^{139}\) Genetic information falls into the category of intimate personal data. As discussed, the DNA of one family member can be used to reveal information about kinship, hereditary disorders and genetic predispositions of the entire family, none of which is typically accessible to the public. Thus, Favish supports protecting individuals’ privacy interest in their family member’s DNA because of the intimate personal data contained within that DNA.

Fourth, Favish can be read to support finding that individuals have a privacy interest in information about their family members that subjects them to unwanted scrutiny. Although this was not the explicit basis for the decision in Favish, concern that Foster’s family members would be subjected to unwanted scrutiny by the release of the pictures may have animated the Court’s decision. This reading of Favish is supported by the Court’s quotation of Sheila Foster Anthony’s sworn declaration opposing disclosure based on her fear of unwanted scrutiny. In her sworn declaration, Sheila Foster Anthony, Foster’s sister, wrote that she opposed the disclosure because “I fear that the release of [additional] photographs certainly would set off another round of intense scrutiny by the media . . . Once again my family would be the focus of conceivably unsavory and distasteful media coverage.”\(^{140}\)

There is significant evidence that the collection of DNA from one member of a family may subject the entire family to unwanted scrutiny. In the case of familial searching, the identification and analysis of partial DNA matches subjects family members to genetic surveillance. The current inaccuracy associate with familial searching also means that relatives of convicted persons already in the system are much more likely to be a suspect for a crime they did not commit.

Although the source of protection for family members’ privacy stemmed from Exemption 7 of the FOIA, the privacy interest itself exists separately from that legislation. The Court did not find that Exemption 7 created a personal privacy interest for family members, but instead found that Exemption 7 protects the freestanding privacy interest individuals enjoy in information about their family members.

The Supreme Court, however, has found that “[t]he question of the statutory meaning of privacy under the FOIA is . . . not the same as the question whether a tort action might lie for invasion of privacy or the question whether an individual’s interest in privacy is protected by the Constitution.”\(^{141}\) Thus, while Favish identifies individuals’ privacy interest in information about their family members, Favish does not clearly support the proposition that this privacy interest is protected by the Constitution.

\(^{139}\) 541 US at 166.

\(^{140}\) Id at 167.

c) Borough of Barrington: Informational family privacy. In Doe v Borough of Barrington, the family members of an HIV-positive man claimed that the government’s disclosure of their husband’s and father’s HIV status to their neighbors violated their Fourteenth Amendment right to privacy. The court agreed. The court found that the “[d]isclosure of a family member’s medical condition, especially exposure to or infection with the AIDS virus, is a disclosure of a ‘personal matter’” that is protected by the Fourteenth Amendment.

In deciding to extend Fourteenth Amendment privacy protection to the HIV-positive person’s family members the court reasoned that:

[t]he hysteria surrounding AIDS extends beyond those who have the disease. The stigma attaches not only to the AIDS victim, but to those in contact with the AIDS patients. Revealing that one’s family or household member has AIDS causes the entire family to be ostracized. The right to privacy in this information extends to members of the AIDS patient’s immediate family. Those sharing a household with an infected person suffer from disclosure just as the victim does. Family members, therefore, have a substantial interest in keeping this information confidential.

The court went on to determine that the government’s interest in disclosure did not outweigh the family member’s substantial privacy interest.

One of the defendants argued that the family members did not have standing to bring the action because only the HIV-positive person’s privacy rights were violated. The court found this argument unpersuasive because the Plaintiffs did not assert the constitutional rights of [their HIV-positive family member]. [Plaintiff] sues as guardian for her minor children for the violation of their own rights to privacy. The children have standing to sue for the violation of their right to privacy from governmental disclosure of their father’s infection with AIDS. Likewise [plaintiff] individually asserts a violation of her constitutional right to privacy. That the officer did not reveal information about the children’s own medical condition is immaterial. A family member’s diagnosis with AIDS is a personal matter, as defined in Whalen v. Roe, that falls within the protection of the Constitution.

d) Borough of Barrington: Analysis and application. Borough of Barrington supports family privacy interests relevant to DNA indexing generally and familial searching specifically

\[142\] 729 F Supp 376 (DNJ 1990).
\[143\] Id at 382.
\[144\] Id at 384 (internal citations omitted).
\[145\] Id.
\[146\] Id at 379.
\[147\] Id at 386.
in three important ways. First, in *Borough of Barrington* the court found that family members have a Fourteenth Amendment privacy interest, as defined in *Whalen v Roe*, in one another’s medical conditions. As already discussed, DNA contains vast amounts of medical information, including the existence of certain types of genetic conditions and predispositions. Thus, *Borough of Barrington* supports finding family members have a privacy interest in one another’s DNA because that DNA contains medical information.

Second, as in *Favish*, in *Borough of Barrington* the court found that family members have a privacy interest in information that the government legally obtained. This indicates that family members do not lose their privacy interest in information simply because the government comes into possession of it. Therefore, *Borough of Barrington* supports protecting individuals’ privacy interest in their family members’ genetic information legally collected under DNA indexing statutes.

Third, the court in *Borough of Barrington* focused on the fact that the AIDS stigma extends beyond the infected persons and can cause their family members to be ostracized. This indicates the court was concerned about the very real impact disclosure had on the AIDS patient’s family members. Disclosing that the plaintiffs’ husband and father had AIDS communicated information about the plaintiffs that caused ostracism in their community. Thus, the court found family members’ privacy interest in one another’s medical conditions was especially strong in the case of AIDS. Family members’ privacy interest in one another’s DNA is similarly strong because the collection of DNA from one member of a family communicates information about the entire family and has the very real impact of subjecting the entire family to lifelong genetic surveillance. Therefore, *Borough of Barrington* supports finding family members possess a particularly robust privacy interest in one another’s DNA because of the sensitive information contained therein.

In sum, various legal sources support finding that individuals have a privacy interest in their family members’ DNA. As discussed above, state genetic privacy statutes and various court decisions support finding individuals have a robust privacy interest in their own genetic information. *Favish* and *Borough of Barrington* support extending this privacy interest to genetic information obtained not only from an individual’s own DNA, but also from that of a family member.

B. Familial Searching as a Fourth Amendment Search

Familial searching is the identification and analysis of partial DNA matches for the purpose of identifying family members of persons profiled in CODIS. This potential search occurs not when the DNA is collected from convicted persons, but when it is subsequently analyzed in potentially impermissible ways.

---

148 Although the court found the privacy interest especially strong in the context of HIV status, it found such a privacy interest was not limited to cases involving HIV status. See id at 382.

149 Id at 384.
The Supreme Court has held that where “the Government seeks to obtain physical evidence from a person, the Fourth Amendment may be relevant at several levels.”\(^{150}\) In \textit{Skinner},\(^{151}\) the Supreme Court evaluated a Fourth Amendment challenge to drug and alcohol tests for railroad workers.\(^{152}\) The Court found that aside from the “initial detention necessary to procure the evidence . . . [o]btaining and examining evidence may also be a search if doing so infringes an expectation of privacy that society is prepared to recognize as reasonable.”\(^{153}\) The Court found that aside from the obvious physical intrusion from the collection of blood, “[t]he ensuing chemical analysis of the sample to obtain physiological data is a further invasion of the tested employee’s privacy interests.”\(^{154}\) \textit{Skinner} supports finding certain kinds of analysis (those which create a further invasion of privacy) constitute separate Fourth Amendment searches.

In the context of DNA indexing, several courts have found that the ensuing analysis of the DNA is a far greater invasion of privacy than the actual collection of the physical sample. In \textit{Amerson}, the Second Circuit found that the “analysis and maintenance of [offenders’] information”\(^{155}\) constituted a “potentially much more serious invasion of privacy” than the actual physical intrusion.\(^{156}\) In \textit{Kincade}, Judge Kozinski dissented from the opinion, stressing that “[i]t is important to recognize that the Fourth Amendment intrusion here is not primarily the taking of the blood, but the seizure of the DNA fingerprint and its inclusion in a searchable database.”\(^{157}\)

This point is especially salient in the context of familial searching. Although family members of the individual from whom the DNA was collected have not had any physical intrusion into their bodies, the government can analyze that individual’s genetic information in ways that no longer search for the person from whom it was obtained (no exact match exists), but instead search for their family members (by identifying and analyzing partial matches). This second search that is consciously directed at convicts’ family members invades their reasonable expectation of privacy because it allows the government to genetically monitor them in otherwise impossible ways.

As previously discussed, individuals have a robust privacy interest in their genetic information. Family privacy law suggests that individuals’ privacy interest in their genetic information should extend to include information obtained not only from their own DNA, but also from the DNA of their family members. Without Fourth Amendment protection, the government could track family members (and even indicate the type of family relation) with near-exact accuracy. This invasion of privacy is nearly identical to a search for exact matches, which many courts consider a more serious invasion of privacy than the initial collection of DNA. Thus, familial searching violates family members’ reasonable expectation of privacy.

\(^{151}\) Id.
\(^{152}\) Id at 606.
\(^{153}\) Id at 616 (internal citations omitted).
\(^{154}\) Id.
\(^{155}\) Nicholas, 430 F3d at 670.
\(^{156}\) Amerson, 483 F3d at 85.
\(^{157}\) Kincade, 379 F3d at 873 (Kozinski dissenting).
Although it might initially appear radical to find that the subsequent use of convicts’ DNA can infringe upon the Fourth Amendment rights of their family members, conceptualizing familial searching as a Fourth Amendment search comports with Fourth Amendment doctrine. In the sections below, this Comment analyzes evolving Fourth Amendment doctrine as it relates to the exceptional characteristics of DNA generally and familial searching specifically. Based on this analysis, this Comment finds that Fourth Amendment doctrine supports finding that familial searching constitutes a Fourth Amendment search of convicts’ family members.

1. Subsequent use.

Since the passage of the Bill of Rights, Fourth Amendment doctrine has shifted from a property-based to a privacy-based approach. As discussed, early Fourth Amendment cases focused on whether evidence was collected from a “constitutionally protected area.” However, in *Katz*, the Court announced that “the Fourth Amendment protects people, not places.” Post-*Katz*, a Fourth Amendment search occurs when the collection of evidence violates an individual’s reasonable expectation of privacy.

Familial searching constitutes a separate Fourth Amendment search of convicted persons’ family members because the government does not have the power to use property or information, once seized, however it wishes. Prior to the switch from a property-based to a privacy-based Fourth Amendment doctrine, the “government’s possessory interest justifying the initial seizure overrode any objection to subsequent uses.” Because the government was deemed to have a superior property right to the evidence seized (justifying the initial search or seizure) they could use that property as they wished. As discussed below, however, the government was limited to seizing only “instrumentalities of crime, fruits of crime, or contraband” because these were the only types of property to which the government could claim a superior right.

The shift to a privacy-based doctrine in *Katz*, however, completely changed that justification. “Because the original seizure no longer extinguishes all property or privacy rights of the individual, government authorities violate the Fourth Amendment if they use property or information unreasonably even when lawfully obtained.” This should mean that when unreasonable use of lawfully obtained evidence violates an individual’s reasonable expectation of privacy, the government conducts a separate Fourth Amendment search.

Courts have recognized limits on the government’s ability to use properly collected evidence in certain ways. For instance, in *United States v Carey*, police obtained a warrant to

---

160 Id at 351.
161 Henderson, 56 Mercer L Rev at 517 (cited in note 70).
163 Id at 59.
164 Id at 60.
165 172 F3d 1268 (10th Cir 2000).
search a computer for evidence of illegal drug distribution. When an officer discovered a pornographic file, he began searching for other pornographic material. The court held that although the computer was lawfully obtained, searching for the pornographic files amounted to an expansion of the scope of the search, and was illegal without the obtainment of a second warrant.¹⁶⁶

Likewise, when the government obtains convicts’ DNA, the scope of the search should be limited to exact matches, based both on the special needs justification (identification of convicts) and the general balancing justification (convicts’ reduced expectation of privacy). When the government expands that search to identify and analyze partial matches, it exceeds the scope of the search authorized by either the special needs test, or alternatively the general balancing test. Like in Carey, familial searching represents a separate search, outside the scope of the initial search. A privacy-based conception of the Fourth Amendment should prohibit the government from using information, once seized, in ways that violate distinct privacy interests, unless those usages are also shown to be constitutionally reasonable.

2. Role of technology.

Technology has been credited for the shifting emphasis in Fourth Amendment doctrine from property-based to privacy-based protection.¹⁶⁷ Along with this shift, came a parallel shift in the type of evidence police could seize. Prior to 1967, law enforcement agencies were prohibited from seizing “mere evidence” of a crime, and were limited to seizing “instrumentalities of crime, fruits of crime, or contraband.”¹⁶⁸ However, in Warden v Hayden¹⁶⁹ the Court dispensed with the “mere evidence” restriction, and allowed the seizure of clothing fitting the description of those worn by the perpetrators.¹⁷⁰ The Court found that the new privacy-based Fourth Amendment analysis permitted the seizure of “mere evidence” because “privacy is disturbed no more by a search directed to a purely evidentiary object than it is by a search a search directed to an instrumentality, fruit, or contraband.”¹⁷¹

DNA is “mere evidence” of a crime, as it cannot fall into the categories of instrumentalities,¹⁷² fruits¹⁷³ or contraband.¹⁷⁴ Therefore, prior to 1967, the government would not have been able to collect a person’s DNA for evidentiary purposes. Although the shift from property-based to privacy-based conceptions of the Fourth Amendment provided protection to

¹⁶⁶ See also State v Schroeder, 613 NW2d 911 (Wis App 2000) (search for pornographic material was upheld because the police obtained a second warrant for the additional search of the computer).
¹⁶⁷ See, for example, Krent, 74 Tex L Rev at 57 (cited in note 162); Henderson, 56 Mercer L Rev at 511 (cited in note 70).
¹⁶⁸ Krent, 74 Tex L Rev at 59 (cited in note 162).
¹⁷⁰ Id at 310.
¹⁷¹ Id at 301–302.
¹⁷² A weapon would be an example of an instrumentalities.
¹⁷³ Money would be an example of a fruit.
¹⁷⁴ Drug paraphernalia would be an example of contraband.
individuals in areas that had previously been uninhibited by Fourth Amendment constraints, the shift also expanded the government’s power to search and seize a much greater range of evidence.\textsuperscript{175} It would be a mistake, therefore, to permit the collection of DNA based on a privacy-based conception of the Fourth Amendment (as mere evidence), but prohibit its protection based on a property-based conception of the Fourth Amendment (because the DNA seized is not the property of convicts’ family members). The history of the Fourth Amendment’s evolution, as well as technology’s role in shifting the doctrine, support adopting a flexible approach when applying the Fourth Amendment to new technologies, such as familial searching.

In dealing with technological advancements, the Court has had to grapple with how the Fourth Amendment applies to “novel technologies not available to, and perhaps not even conceivable to, the Framers.”\textsuperscript{176} In\textit{Kyllo v United States},\textsuperscript{177} the Court refused to allow the use of new technology to obtain information regarding the interior of a home that “could not otherwise have been obtained without physical intrusion into a constitutionally protected area.”\textsuperscript{178} In order to assure the preservation of the “degree of privacy against government that existed when the Fourth Amendment was adopted,” the Court found the use of new technology to obtain information otherwise protected by the Fourth Amendment constituted a search—“at least where (as here) the technology in question is not in general public use.”\textsuperscript{179}

This analysis supports finding that familial searching represents a search of convicted persons’ immediate family members. Collecting DNA for the purpose of obtaining information about genetic identity is subject to Fourth Amendment protection.\textsuperscript{180} Therefore, using new technology to obtain information about genetic identity should also be considered a Fourth Amendment search. Additionally, the technology here—DNA indexing—qualifies as “technology not in general public use.”\textsuperscript{181} Kyllo supports protecting information (genetic identity) from government use when new technology (familial searching) allows the government to obtain information previously subject to Fourth Amendment constraints.\textsuperscript{182}

3. \textbf{Voluntariness.}

Often the existence of a reasonable expectation of privacy rests heavily on whether an individual has voluntarily shared the information in question with others. The Fourth

\begin{itemize}
  \item \textsuperscript{175} Krent, 74 Tex L Rev at 59 (cited in note 162).
  \item \textsuperscript{176} Henderson, 56 Mercer L Rev at 511 (cited in note 70).
  \item \textsuperscript{177} 533 US 27 (2001).
  \item \textsuperscript{178} Id at 34.
  \item \textsuperscript{179} Id.
  \item \textsuperscript{180} See, for example, Kincade, 379 F3d at 830; Amerson, 483 F3d at 78; Green, 354 F3d at 677–78; Kimler, 335 F3d at 1146.
  \item \textsuperscript{181} Kyllo, 533 US at 34. The technology at issue in Kyllo was infrared technology. Id at 29. The Court has never set forth a standard for determining what constitutes “in general public use” but infrared technology is (and was) much more publicly available than DNA indexing and low-stringency analysis (familial searching). Thus, it would be highly unlikely that a court would find familial searching is in general public use.
  \item \textsuperscript{182} Id at 34.
\end{itemize}
Amendment generally permits the use of information obtained from one party that reveals information about another party. For instance, emails, letters, or lists of telephone calls when rightfully seized from one individual, may allow police to obtain information about others. The ability of the police, however, to obtain information in this fashion seems unquestionable based on the “third party doctrine.”\footnote{See, for example, \textit{Smith}, 442 US at 743–44 (an individual has “no legitimate expectation of privacy in information he voluntarily turns over to third parties”).}

But DNA defies easy classification because of the unique way in which family members involuntarily share genetic information. These “third party” examples are not analogous, because letters, emails, and telephone calls are voluntary transactions, and decisions regarding the government’s collection of these items have relied on the voluntary release of information into the public domain.\footnote{See id; consider Henderson, 56 Mercer L Rev at 519–22 (cited in note 70) (discussing the “Third Party Doctrine” as it relates to encrypted email).} With DNA, individuals make no voluntary choice. My brother will carry my DNA everywhere he goes for the rest of his life. I have not agreed to this arrangement. I have released nothing into the public domain. Our joint possession of one another’s DNA is entirely involuntary.

Fourth Amendment law places great emphasis on this voluntary/involuntary distinction. In \textit{Katz}, Justice Stewart, writing for the majority, explained the importance of this distinction: “What a person knowingly exposes to the public, even in his home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”\footnote{389 US at 351 (internal citations omitted).} This indicates that what family members seek to preserve as private (their DNA) should be constitutionally protected even though the government might have the power to technologically exploit the involuntary sharing relationship among family members.

The Supreme Court has consistently upheld this voluntary/involuntary distinction in a variety of contexts. \textit{In United States v Miller,} the Court held that a bank depositor has no “legitimate ‘expectation of privacy’” in financial information “voluntarily conveyed to . . . banks and exposed to their employees in the ordinary course of business.”\footnote{425 US 435 (1976).} Similarly, in \textit{Smith v Maryland,} the Court found the defendant had no reasonable expectation of privacy in the phone numbers he dialed because he voluntarily conveyed that information to the telephone company.\footnote{Id at 442.} The Court has also refused Fourth Amendment protection for information voluntarily exposed to the plain view of the public\footnote{442 US 735 (1979).} as well as for “a wrongdoer’s misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.”\footnote{Id at 745.}

\footnote{In \textit{Florida v Riley}, 488 US 445 (1989), the Court allowed the government to use evidence obtained by flying over the defendant’s premises, where he grew marijuana in the backyard. The Court found that although the marijuana was hidden from plain view at ground level, the}
These cases illustrate the importance of the voluntary/involuntary distinction. In the case of sisters, neither sister chooses to expose her DNA to the other, nor to the public. Thus, individuals maintain a privacy interest in their genetic information, even though they involuntarily share it with their family members. When the government exploits this involuntary relationship through familial searching, it violates family members’ reasonable expectation of privacy.

4. Control.

For family members to successfully assert a Fourth Amendment challenge to familial searching, they must prove that familial searching violates their reasonable expectation of privacy. At first blush, determining that one person can have a privacy interest in the property of another may seem like an unnatural extension of Fourth Amendment law, but Fourth Amendment case law has long provided this type of protection. In Minnesota v Olsen,\textsuperscript{192} the Court held that an overnight guest has a reasonable expectation of privacy in his or her host’s home.\textsuperscript{193} The Court found that overnight guests enjoy this reasonable expectation of privacy “despite the fact that they have no legal interest in the premises and do not have the legal authority to determine who may or may not enter the household.”\textsuperscript{194} The Court found that the host, in allowing the guest to share his home for the night, is also sharing his privacy.\textsuperscript{195} “That the guest has a host who has ultimate control of the house is not inconsistent with the guest having a legitimate expectation of privacy.”\textsuperscript{196}

Therefore, the Court permits not only that individuals share reasonable expectations of privacy in the same locations and objects, but also that individuals share these reasonable expectations of privacy even when one individual has a greater legal interest or right of control. This is analogous to family members sharing a reasonable expectation of privacy in one another’s DNA. Although the individual from whom the DNA has been collected has the greatest legal interest in, and ultimate control of, his DNA, his immediate family members also possess a reasonable expectation of privacy in his DNA because it reveals information about the entire family that would not typically be discoverable by third parties. Notably, an overnight guest voluntarily chooses to stay in his host’s home for the night, and therefore chooses to share his host’s privacy. Family members, as discussed, have no choice but to share genetic information, so they should have an even stronger expectation of privacy than overnight guests. In the case of familial searching, the government violates this reasonable expectation of privacy

---

\textsuperscript{197} Hoffa v United States, 385 US 293, 302–03 (2006).
\textsuperscript{198} 495 US 91 (1990).
\textsuperscript{199} Id at 98–99.
\textsuperscript{200} Id at 99.
\textsuperscript{201} Id.
\textsuperscript{202} Id; see also Katz, 389 US 347 (finding that an individual had a reasonable expectation of privacy in a public telephone booth, over which he exhibited absolutely no possessory or proprietary interest).
by using convicts’ DNA to obtain otherwise indiscernible information about their family members.

5. Unfit analogies.

DNA’s unique qualities make it difficult to classify. In an attempt to properly conceptualize familial searching, some have analogized it to familiar situations or law enforcement techniques. As discussed below, these analogies are problematic because they fail to take into account these unique qualities.

a) Family resemblance. Some supporters of familial searching have claimed it is analogous to family resemblance.197 One group of scholars argue:

If a witness said that a person in a photograph was not the perpetrator but looked very much [like] him – ‘could have been his brother’ – there seems no reason to think the police could not try to find out whether the pictured man had a brother. Family forensic DNA is a molecular version of this kind of family resemblance.198

This analysis misses a crucial distinction between regular family resemblance, visible to the entire world, and molecular family resemblance, which is not visible for the world to see. As discussed in Kyllo, it has long been the law that “the eye cannot . . . be guilty of trespass.”199 Therefore, observing family resemblance—which is plain for the whole world to see—can hardly be considered a search. But a molecular version of family resemblance is not exposed to the world. Law enforcement agencies are only able to observe such a family resemblance through advanced and developing technological techniques. Therefore, family resemblance fails as a suitable analogy.

b) Fingerprinting. Similarly, DNA indexing is often compared to fingerprinting.200 Although detaining a person to obtain their fingerprints is subject to Fourth Amendment requirements,201 taking fingerprints themselves is not afforded Fourth Amendment protection.202 There are several important distinctions between fingerprinting and DNA indexing. First, unlike fingerprint collection, courts have determined that DNA collection does implicate the Fourth

---

197 Greely, 34 JL Med & Ethics at 257 (cited in note 9).
198 Id.
199 Kyllo, 533 US at 32 (quoting Boyd v United States, 116 US 616, 628 (1886)).
200 See, for example, Nat’l Comm’n on the Future of DNA Evidence, US Dep’t of Justice, Using DNA to Solve Cold Cases 5 (2002) (comparing DNA analysis to fingerprint evidence); Richard Willing, White House Seeks to Expand DNA Database, USA Today 13A (Apr 16, 2003) (quoting Assistant United States Attorney General Deborah Daniels as saying, “DNA is to the 21st century what fingerprinting was to the 20th”).
201 See Davis v Mississippi, 394 US 721 (1969).
202 See United States v Dioniso, 410 US 1, 15 (1973) (stating that fingerprinting “involves none of the probing into an individual’s private life and thoughts that marks an interrogation or search” (internal quotations omitted)).
Amendment. Second, fingerprints, unlike DNA, have limited identification value. At the very least, even so-called “junk DNA” that scientists currently believe lacks significant genetic material, is capable of identifying not only the individual from who it came, but also family connections. Fingerprinting lacks this “molecular family resemblance.” It would be impossible to track a person based on her sibling’s fingerprint. This distinctive quality makes fingerprinting an inappropriate analogy for analyzing familial searching.

VI. THE SPECIAL-NEEDS TEST

If the familial searching constitutes a Fourth Amendment search of convicted persons’ family members, then that search is subject to the reasonableness requirement of the Fourth Amendment. The search of the convicted person’s family members, like the search of the convicted person, is both warrantless and lacks individualized suspicion. Additionally, the general balancing test applies only to searches of parolees and conditional releasees. Because the family members are presumably not parolees or conditional releasees themselves (if they were, they would already be in the system and the government could obtain a direct match), the general balancing test cannot apply. Consequently, the special-needs test must be conducted to analyze the constitutionality of familial searching.

The special-needs test requires analysis of 1) “whether the search and seizure is justified by a special need beyond the ordinary needs of normal law enforcement,” and 2) “whether the search was reasonable in light of that special need.” The three circuits that have approved of DNA indexing based on the special-needs test have based their decisions on the convicted person’s greatly reduced expectation of privacy. The privacy interest of these family members, who have not forfeited any of their privacy rights, could potentially be potent enough to prohibit familial searching.

A. Familial Searching: Existence of a Special Need

If familial searching represents a search of convicted persons’ family members, it is clear no special need exists. As discussed, in Edmund the government used motor vehicle checkpoints in an effort to detect illegal narcotics trafficking. The Supreme Court found that because the primary purpose of the checkpoint was to “detect evidence of ordinary criminal wrongdoing” no special need existed.

Similarly, in Ferguson v City of Charleston a state hospital collected urine samples from pregnant women in order to drug test them for cocaine use without their consent. The

---

203 See, for example, Amerson, 483 F3d at 78; Green, 354 F3d at 677-78; Kimler, 335 F3d at 1146; Sczubelek, 402 F3d at 184; Groceman, 354 F3d at 413; Kincade, 379 F3d at 832.
204 See Amerson, 483 F3d at 80.
205 Id.
206 Id.
207 531 US at 42.
209 Id at 70–76.
hospital then turned positive results over to police officers, who arrested the women, unless they consented to substance abuse treatment. The Court found the searches were unconstitutional because their primary purpose was to collect evidence for law enforcement purposes.

When the government analyzes DNA found at a specific crime scene against DNA found in CODIS, it is performing that partial-match analysis for the purpose, like in Edmond, of obtaining evidence of ordinary criminal wrongdoing. Furthermore, the partial-match analysis, like in Ferguson, is being done to collect evidence for law enforcement purposes. In all three cases the government lacks a special need.

Familial searching, like the searches in Edmond and Ferguson, is distinct from typical special-needs exceptions. Often special needs identified by the Supreme Court revolve around health or safety. For instance the Supreme Court has upheld sobriety checkpoints designed to improve road safety, searches at airports and entrances of courthouses and buildings designed to ensure public safety, searches of inmates designed to ensure institutional safety, inspections to monitor compliance with building safety codes designed to ensure public safety, and random drug tests of students and employees in a variety of contexts, also designed to ensure health and safety. Familial searching is notably distinct from these types of searches.

As previously discussed in Part III, the existence of a special need for DNA indexing statutes is unclear. However, courts that have upheld the existence of a special need have found that “[a]lthough the state’s DNA testing of inmates is ultimately for a law enforcement goal,” it falls within the special-needs exception because “it is not undertaken for the investigation of a specific crime.” Familial searching is done squarely for the purpose of investigating a specific crime. Thus, no special need for familial searching exists. Therefore, familial searching is unconstitutional if it represents a search of a convicted person’s family members.

If familial searching constitutes a search, a like argument could be made about searching for exact matches. Just as for family members, if searching for an exact match represents a search, then the search is for ordinary law enforcement purposes. Thus, no special need would exist at the time of that search. Therefore, the special-needs test could not justify the use of DNA indexing. Currently, however, the majority of circuits that have considered DNA indexing statutes have adopted the general balancing test. If this test is appropriate, then the existence of a special need is unnecessary, because the search would still be of convicted persons. Thus, courts could justify allowing the search of DNA databanks for exact, but not partial, matches.

---

210 Id at 72.
211 Id at 83.
214 See Bell v Wolfish, 441 US 520 (1979).
215 Camara v Mun Ct of SF, 387 US 523 (1967).
217 Green, 354 F3d at 678.
218 Id.
VII. Familial Searching as a Constitutionally Unreasonable Use

A number of circuit courts that have upheld the constitutionality of DNA indexing statutes based on convicts’ Fourth Amendment challenges have remarked that if the DNA extracted from inmates were used for purposes other than their future identification, a new analysis would be necessary. Familial searching clearly represents an appropriate opportunity to reexamine the validity of DNA indexing statutes.

As discussed, all Fourth Amendment searches must be constitutionally reasonable. The reasonableness of a search is based on three factors: (1) the nature of the privacy interest involved; (2) the character and degree of the governmental intrusion; and (3) the nature and immediacy of the government’s needs, and the efficacy of its policy in addressing those needs.220 

In Amerson, the court noted that it was “mindful of the vast amount of sensitive information that can be mined from a person’s DNA and the very strong privacy interests that all individuals have in this information,” but found that the federal DNA statute “provides adequate safeguards to insure that the privacy invasion” is minimized.221 First, the court found it was important that the “junk DNA” sequences used to create DNA profiles “are not currently associated with any known physical or medical characteristics.”222 Secondly, the court stressed that “the Act limits the circumstances and purposes for which the DNA profiles can be released and provides significant penalties for any misuse of the DNA samples or profiles.”223 The court found that because “the DNA profile derived from the offender’s blood sample establishes only a record of the offender’s identity,” and convicted felons have a severely diminished expectation of privacy in their identity, the privacy intrusion was small.224

This analysis reveals that the way the government uses DNA bears on the reasonableness of the search.225 Part of the reasonableness inquiry is determining the nature of the invasion of privacy. The invasion of privacy is altered when the government uses the DNA in different ways. For instance, using DNA to establish identity involves a different invasion of privacy than using the DNA to test for AIDS. In addition to altering the privacy interest, “the state’s intended use also affects the magnitude of the state’s interest.”226

Fourth Amendment scholars have noted that “[b]ecause the original seizure no longer extinguishes all property or privacy rights of the individual, government authorities violate the

219 See, for example, Amerson, 483 F3d at 85 n. 13; Kincade, 379 F3d at 838; Nicholas, 430 F3d at 670–71.
220 Cassidy, 471 F3d at 75.
221 Id at 85.
222 Id.
223 Id.
224 Id at 86.
225 See also Krent, 74 Tex L Rev at 63–64 (cited in note 162).
226 Id at 64.
Fourth Amendment if they use property or information unreasonably even when lawfully obtained.” 227 Harold Krent contends that the reasonableness of a search depends partially on what will be done with the evidence after it has been obtained. 228 Thus, Krent advocates invalidating searches when their intended use is constitutionally unreasonable. 229 As discussed, a strong argument can be made that familial searching violates family members’ reasonable expectation of privacy. This suggests that familial searching should be considered a constitutionally unreasonable intended use.

Currently, familial searching is a relatively rarely used technique. This may be partially because the current number of CODIS markers does not facilitate scientifically exact familial searching. The government does, however, have the ability to increase the number of CODIS markers to make familial searching significantly more accurate. The recent expansion of DNA databases suggests the government is moving in the direction of trying to genetically monitor a greater portion of the population. This trend is supported by the FBI’s new policy, which facilitates familial searching and will likely increase its frequency. Both of the above factors suggest the United States may be moving in the direction of the United Kingdom, which has the “largest domestic forensic DNA database per capita in the world.” 230 In the United Kingdom, familial searching is a much more commonly used law enforcement technique. 231

Based on its increasing use, familial searching represents an appropriate opportunity to reexamine the validity of DNA indexing statutes. The above analysis suggests familial searching should be considered a constitutionally unreasonable use. As a result, the continuing practice of familial searching threatens to invalidate DNA indexing laws.

VII. CONCLUSION

Given the increasing use of familial searching, as well as the FBI’s current policy on partial DNA matches, familial searching is likely to become an important legal topic in the coming years. This Comment has put forth two potential ways in which family members could seek protection via the Fourth Amendment.

Overall, this Comment’s analysis supports two central propositions: 1) individuals have a reasonable expectation of privacy in their family members’ DNA and 2) that privacy interest should curtail the government’s use of convicted persons’ DNA and prohibit familial searching.

227 Id at 60.
228 Id at 49.
229 Id.
231 See, for example, Frederick R. Bieber, Turning Base Hits Into Earned Runs: Improving the Effectiveness of Forensic DNA Data Bank Programs, 34 JL Med & Ethics 222, 226 (Summer 2006).