



DNA Databanking: Selected Fourth Amendment Issues and Analysis

Emily C. Barbour
Legislative Attorney

June 6, 2011

Congressional Research Service

7-5700

www.crs.gov

R41847

Summary

Over the past few decades, state and federal lawmakers have promoted the development of databases containing DNA (deoxyribonucleic acid) profiles for individuals who are under the supervision of the criminal justice system due to their known or suspected involvement in a felony or other qualifying crime. Congress has demonstrated concern toward some aspects of DNA databanking by requiring expungement of a DNA profile in certain circumstances, prohibiting most non-forensic uses of DNA profiles and databases, and restricting familial searching. However, in general, Congress has taken a supportive attitude toward DNA databanking and has incentivized the development, expansion, and integration of DNA databases.

As DNA database programs have widened in scope and grown in numbers, their consistency with the Fourth Amendment's prohibition on unreasonable searches and seizures has increasingly been challenged. In the context of compulsory DNA collection, courts have widely upheld laws mandating the collection of DNA from persons who were convicted and are subject to the penal system's custody or supervision. However, no judicial consensus has emerged regarding the constitutionality of mandating DNA collection from arrestees who have been criminally indicted. Instead, courts have split over the existence and scope of an arrestee's reasonable expectation of privacy and the degree of privacy intrusion caused by DNA sampling. The limited number of court decisions in this area also suggests that there are conflicting opinions about the analogousness of DNA collection and fingerprinting.

Courts have generally upheld the indefinite use and storage of a lawfully databanked DNA profile after its source's conviction. However, not all courts agree that *any* post-conviction use of those profiles is constitutionally acceptable. In particular, observers are now raising questions about the Fourth Amendment consistency of using databases for non-forensic purposes and for familial searching—that is, using the DNA databases to locate potential relatives of an unidentified suspect. Currently, these concerns are largely confined to the scholarly literature—they have not come before a federal court—and are primarily centered on state database programs. Unlike some state DNA databases, the National DNA Index System (NDIS) and the Combined DNA Index System (CODIS) can not be used for either non-forensic research or intentional familial searching. However, the increase in states that authorize familial searching suggests that it may not be long before the constitutionality of familial searching comes before a federal court.

As these issues percolate up to the courts, new advances and revelations in the science of forensic analysis and databanking may have potentially significant legal implications. Several courts have suggested that new forensic techniques and scientific findings would require them to reevaluate their legal conclusions and analysis. In particular, research into the scope and nature of the information revealed by the “junk” DNA used in forensic analysis may alter how courts measure the intrusiveness of DNA profiling if it suggests that “junk” DNA reveals more sensitive information about its source than scientists previously thought.

Contents

Introduction	1
Background on Law Enforcement Use of DNA	2
Statutory Framework.....	4
Expansion of Statutory Authorities for DNA Profiling	5
Expungement Provisions	7
Fourth Amendment Overview	8
Search or Seizure	8
“Reasonableness” Inquiry When the Fourth Amendment Applies	9
Collecting DNA	10
Prisoners, Parolees, Probationers, and Supervised Releasees.....	11
Arrestees	12
Using and Retaining Databanked DNA	14
Post-Sentence Privacy Rights	14
Informational Privacy Rights.....	16
Academic Research and Non-forensic Information	16
Familial Searching and Information About Genetic Relationships.....	17
Implications of New Research on Junk DNA.....	18
Conclusion.....	19

Contacts

Author Contact Information	20
Acknowledgments	20

Introduction

In recent years, state and federal laws have facilitated law enforcement's expanded use of deoxyribonucleic acid (DNA) for investigating and prosecuting crimes.¹ These laws authorize compulsory collection of biological matter, which local law enforcement agencies send to the Federal Bureau of Investigation (FBI) for analysis. The FBI then stores unique DNA profiles in a national distributive database, through which law enforcement officials match individuals to crime scene evidence.

Early laws authorized compulsory extraction of DNA only from people convicted for violent or sex-based felonies, such as murder, kidnapping, and offenses "related to sexual abuse"—crimes associated with historically high recidivism rates and for which police were likely to find evidence at crime scenes.² However, in recent decades, new laws have greatly extended the scope of compulsory DNA collection, both by expanding the range of offenses triggering collection authority and, more recently, by authorizing compulsory collection from people who have been arrested but not convicted.

Opponents of DNA databases suggest that DNA databases are "Orwellian" because of the amount of information about private citizens that they put into the control of the government.³ The most frequent criticism is that the programs violate the Fourth Amendment to the U.S. Constitution.⁴ Several federal courts have heard cases alleging that it is unconstitutional for an individual's pre- or post-trial release to be conditioned on DNA collection. Another Fourth Amendment argument, albeit a less litigated one, contends that it is unconstitutional to permit the use of databanked DNA profiles for purposes other than identifying a genetic match with a suspect.

The Fourth Amendment protects individuals' privacy from unreasonable searches and seizures by the government. Federal courts have generally held that compulsory DNA collection from a person who has been convicted of a felony or other qualifying crime and placed under the supervision of the criminal justice system does not constitute an unreasonable search under the

¹ For more on the progression of federal legislation authorizing use of DNA, see CRS Report R41800, *DNA Testing in Criminal Justice: Background, Current Law, Grants, and Issues*, by Nathan James.

² For example, offenses triggering DNA collection authority under the original DNA Analysis Backlog Elimination Act of 2000, P.L. 106-546 (2000), included murder, voluntary manslaughter, and other offense relating to homicide; offenses relating to sexual abuse, sexual exploitation or other abuse of children, or transportation for illegal sexual activity; offenses relating to peonage and slavery; kidnapping; offenses involving robbery or burglary; certain offenses committed within Indian territory; and attempt or conspiracy to commit any of the above offenses.

³ *Banks v. United States*, 490 F.3d 1178, 1180 (describing the arguments of DNA database critics as allusions "to a police state reminiscent of George Orwell's dystopia portrayed in *1984*"). See, e.g., *United States v. Sczubelek*, 402 F.3d 175, 194 n.11 (3rd Cir. 2005) (McKee, J., dissenting) (characterizing the DNA Act as ushering in an "Orwellian intrusion"); *United States v. Kincade*, 379 F.3d 813, 870 (9th Cir. 2004) (Reinhardt, J., dissenting) ("The compulsory extraction of blood samples and the maintenance of permanent DNA profiles of American citizens is, unfortunately, the beginning not the end. 1984 arrives twenty years later than predicted").

⁴ Litigants have also brought challenges under the Eighth and Fourteenth Amendments to the U.S. Constitution as well as under other legal and constitutional theories. See Hon. Donald E. Shelton, *Twenty-First Century Forensic Science Challenges for Trial Judges in Criminal Cases: Where the Polybutadiene Meets the Bitumen*, 18 WIDENER L. J. 309, 361-62 (2009) (listing different theories used to challenge the constitutionality of DNA database and compulsory collection statutes). See also *United States v. Pool*, 645 F. Supp.2d 903 (9th Cir. 2009) (rejecting challenges under Fourth, Fifth, and Eighth Amendments to the U.S. Constitution). However, this report is limited to a discussion of challenges brought under the Fourth Amendment.

Fourth Amendment.⁵ These courts found that a convicted felon has a diminished expectation of privacy and that DNA profiling is a minimal intrusion into that privacy.⁶ However, as discussed below, the courts have not reached a consensus on the Fourth Amendment consistency of *pre-conviction* DNA collection. Moreover, the courts have not yet had an opportunity to articulate the constitutional limits on how databanked DNA profiles may be used.

This report traces the expansion of the statutory authorities for DNA databases and identifies emerging areas of consensus and discord among the federal courts over the Fourth Amendment consistency of compulsory DNA collection and the use of DNA databases. It also predicts additional Fourth Amendment issues that may come before both Congress and the federal courts in the near future.

Background on Law Enforcement Use of DNA

DNA is a complex molecule found in the nucleus and mitochondria of an organism's cells.⁷ It consists of two strands of nucleotides, the sequence of which contains the information that forms the basis of the human genetic code. The vast majority of human DNA is exactly the same, but small variations in the sequencing of the nucleotides create people's distinguishing characteristics.⁸ Only identical twins share the same DNA profile.⁹

With the help of DNA profiling technology, forensic scientists can examine different regions—or “loci”—of DNA to develop a DNA profile of the person from whom the DNA was extracted.¹⁰ Because forensic analysts examine a select group of loci, the resulting DNA profile may not necessarily be unique to that individual.¹¹ However, advances in technology have enabled analysts to produce increasingly discriminating profiles. Today, the probability that two unrelated individuals would share a DNA profile derived from an uncontaminated sample of DNA from a cell's nucleus is estimated to be one in a billion at most.¹²

⁵ *E.g.*, *United States v. Weikert*, 504 F.3d 1 (1st Cir. 2007); *United States v. Amerson*, 483 F.3d 73 (2^d Cir. 2007), *cert. denied* 552 U.S. 1042 (2007); *Wilson v. Collins*, 517 F.3d 421 (6th Cir. 2006); *United States v. Hook*, 471 F.3d 766 (7th Cir. 2006), *cert. denied* 549 U.S. 1343 (2007); *United States v. Kraklio*, 451 F.3d 922 (8th Cir. 2006), *cert. denied* 549 U.S. 1044 (2006); *United States v. Kriesel*, 508 F.3d 941 (9th Cir. 2007); *United States v. Banks*, 490 F.3d 1178 (10th Cir. 2007); *United States v. Castillo-Lagos*, 147 Fed. App'x 71 (11th Cir. 2005).

⁶ *See, e.g.*, *Weikert*, 504 F.3d at 27, 30-33 (finding that a convicted felon on supervised release “has a substantially diminished expectation of privacy” and collecting a blood sample is a “minimal” intrusion that is not meaningfully augmented by the government's subsequent use of that sample to create and databank a DNA profile); *Amerson*, 483 F.3d at 29 (finding that the appellants have a “diminished” expectations of privacy and the collection of their DNA for a DNA database is a “small” intrusion of privacy).

⁷ For a more in-depth discussion of DNA and its use in law enforcement, see CRS Report R41800, *DNA Testing in Criminal Justice: Background, Current Law, Grants, and Issues*, by Nathan James.

⁸ *See* Human Genome Program, U.S. Department of Energy, *Primer on Molecular Genetics* (Washington, DC, 1992), <http://www.ornl.gov/hgmis/publicat/primer/primer.pdf>.

⁹ *United States v. Kincade*, 379 F.3d 813, 818 n.7 (9th Cir. 2004) (en banc), *cert. denied*, 544 U.S. 924 (2005).

¹⁰ In the United States, forensic scientists use “short tandem repeat” technology to analyze 13 DNA loci. Department of Energy, *Human Genome Project Information: DNA Forensics*, at http://www.ornl.gov/sci/techresources/Human_Genome/elsi/forensics.shtml.

¹¹ NATIONAL POLICING IMPROVEMENT AGENCY, NATIONAL DNA DATABASE ANNUAL REPORT 2007-2009, 7 (2009).

¹² *See id.*; NATIONAL INSTITUTE OF JUSTICE, USING DNA TO SOLVE COLD CASES, 5-7 (2009), available at <http://www.ncjrs.gov/pdffiles1/nij/194197.pdf>.

DNA profiles are often compared to fingerprints.¹³ As with fingerprints, law enforcement officers collect DNA samples from specific classes of individuals, such as prisoners. However, compulsory DNA collection generally entails blood or saliva samples rather than finger impressions, and DNA profiles can later match any of many types of biological matter obtained from crime scenes.¹⁴ For these reasons, DNA matching is considered a complement to, rather than merely a supplement for, fingerprint analysis in identifying criminal suspects.¹⁵

The FBI administers DNA storage and analysis for law enforcement agencies across the country. FBI analysts create DNA profiles by “decoding sequences of ‘junk DNA.’”¹⁶ So-called “junk DNA” is the name for DNA loci that are “not presently recognized as being responsible for trait coding.”¹⁷ Because junk DNA is not currently “associated with any known physical or medical characteristics,” its use in forensic analysis prevents, at least for the time being, DNA profiles from containing private or sensitive information about the subject.¹⁸

Typically, a law enforcement agency’s phlebotomist collects a blood or saliva sample from the subject pursuant to state or federal law. The sample may then be analyzed and converted into a DNA profile by a public laboratory (or outsourced by that public lab to a private one) that adheres to the FBI’s Quality Assurance Standards.¹⁹ Assuming the laboratory and analyst that generated the profile are adequately credentialed, the resulting DNA profile may then be entered into the Combined DNA Index System (CODIS).²⁰ CODIS includes DNA profile databases composed at the local, state, and national levels.²¹ At the national level, the National DNA Index System (NDIS) facilitates sharing of DNA profiles among participating law enforcement agencies throughout the United States.²² At each level, profiles are categorized into forensic (crime scene) profiles, offender profiles, and arrestee profiles.²³

¹³ The term “DNA fingerprinting” was coined in 1985. L.A. Foreman et. al., *Interpreting DNA Evidence: A Review*, 71 INT’L STATISTICAL REVIEW 473, 474 (2003) (giving credit to a 1985 article in *Nature* for coining the term). However, the analogy between fingerprinting and DNA profiling has since drawn criticism from both the legal and scientific communities. See, e.g., Foreman, *supra*, at 474 (describing the term “DNA fingerprinting” as “misleading”); *United States v. Mitchell*, 681 F. Supp.2d 597, 608 (W.D. Pa. 2009) (criticizing the comparison as “pure folly”). Given this criticism, a frequently used argument against DNA databases is “genetic exceptionalism”—that is, the theory that DNA profiles are fundamentally different from other types of identification and medical records. George J. Annas, *Genetic Privacy*, in DNA AND THE CRIMINAL JUSTICE SYSTEM: THE TECHNOLOGY OF JUSTICE 135, at 136-37 (David Lazer ed., 2004).

¹⁴ Under federal statute and analogous state laws, officials collect DNA from “tissue, fluid, or other bodily sample.” See 42 U.S.C. § 14135a(c)(1). To facilitate especially “reliable” DNA analysis, FBI guidelines direct federal law enforcement officials to rely on blood samples. See *Kincade*, 379 F.3d at 817.

¹⁵ DNA-Sample Collection and Biological Evidence Preservation in the Federal Jurisdiction, 73 Fed. Reg. at 74933-34.

¹⁶ *Amerson*, 483 F.3d at 76.

¹⁷ *Kincade*, 379 F.3d at 818.

¹⁸ See *id.* at 818, 837 (suggesting that, by virtue of looking only at the subject’s junk DNA, the government’s invasion of the subject’s privacy is minimal); H.R. Rep. No. 106-900 at 27.

¹⁹ JOHN M. BUTLER, FUNDAMENTALS OF FORENSIC DNA TYPING 270 (2010). In addition to signing a memorandum of understanding agreeing to adhere to these standards, state laboratories submitting DNA profiles to the National DNA Index System must also be accredited and audited annually. *Id.* at 271.

²⁰ DNA INITIATIVE, COMBINED DNA INDEXING SYSTEM, <http://www.dna.gov/dna-databases/codis>.

²¹ DNA INITIATIVE, LEVELS OF THE DATABASE, <http://www.dna.gov/dna-databases/levels>.

²² See FEDERAL BUREAU OF INVESTIGATION, COMBINED DNA INDEX SYSTEM (CODIS), <http://www.fbi.gov/about-us/lab/codis/codis>.

²³ DNA Initiative, Levels of the Database, *supra* note 21.

As of March 2011, the National DNA Index (NDIS) contained over 9,535,059 offender profiles.²⁴ The primary metric by which CODIS is evaluated is the number of criminal investigations that CODIS aids.²⁵ As of March 2011, CODIS had assisted more than 135,500 investigations,²⁶ suggesting that between one and two percent of all samples taken from an offender have assisted a criminal investigation.²⁷

Statutory Framework

The categories of individuals from whom law enforcement officials may require DNA samples have expanded in recent years. The federal government and most states authorize compulsory collection of DNA samples from individuals convicted for specified criminal offenses, including all felonies in most jurisdictions and extending to misdemeanors, such as failure to register as a sex offender or crimes for which a sentence greater than six months applies, in some jurisdictions.²⁸ In addition, the federal government and some states now authorize compulsory collection from people whom the government has arrested or detained but not convicted. As amended, the DNA Analysis Backlog Elimination Act 2000, discussed below, authorizes compulsory collection from individuals in federal custody, including those detained, arrested, or facing charges, and from individuals on release, parole, or probation in the federal criminal justice system.²⁹ Under the federal law, if an individual refuses to cooperate, relevant officials “may use or authorize the use of such means as are reasonably necessary to detain, restrain, and collect a DNA sample.”³⁰ State laws vary, but nearly all states authorize compulsory DNA collection from people convicted for specified crimes, and a small but growing number of states also authorize compulsory collection from arrestees.³¹

²⁴ FEDERAL BUREAU OF INVESTIGATION, CODIS—NDIS STATISTICS, <http://www.fbi.gov/about-us/lab/codis/ndis-statistics>.

²⁵ *Id.*

²⁶ *Id.*

²⁷ *See id.* *See also* Michael T. Risher, *Warrantless Collection of DNA From People Merely Accused of a Crime Raises Not Only Privacy Concerns But Also Questions About Efficacy*, 88 CRIM. L. REP. 320 (December 15, 2010) (stating that, according to FBI statistics, the “hit” rate as of September 2010 was 1.4%). The FBI also breaks down the number of offender profiles and investigations aided by state on its website. Federal Bureau of Investigation, CODIS—NDIS Statistics, *supra* note 24. For a more detailed synthesis and overview of studies regarding the utility of DNA databases to criminal investigations, see CRS Report R41800, *DNA Testing in Criminal Justice: Background, Current Law, Grants, and Issues*, by Nathan James.

²⁸ For more information on state laws regarding compulsory DNA collection, see National Conference of State Legislatures, *State Laws on DNA Data Banks: Qualifying Offenses, Others Who Must Provide Sample* (February 2010), at <http://www.ncsl.org/default.aspx?tabid=12737>.

²⁹ 42 U.S.C. § 14135a. *See also* 18 U.S.C. § 3142(b) (“The judicial officer shall order the pretrial release of the person [charged with an offense] ... subject to [inter alia] the condition that the person cooperate in the collection of a DNA sample from the person if the collection of such a sample is authorized pursuant to section 3 of the DNA Analysis Backlog Elimination Act of 2000 ...”).

³⁰ 42 U.S.C. § 14135a(a)(4)(A).

³¹ *See* National Conference of State Legislatures, *State Laws on DNA Data Banks: Qualifying Offenses, Others Who Must Provide Sample* (February 2010), <http://www.ncsl.org/default.aspx?tabid=12737> (indicating 21 states that authorize DNA collection from arrestees). However, many of the state laws authorizing collection from arrestees limit the scope of such collection to people arrested for specified violent or serious crimes.

Expansion of Statutory Authorities for DNA Profiling

At the federal level, statutory authority for compulsory DNA collection has expanded relatively rapidly. During the 1990s, a trio of federal laws created the logistical framework for DNA collection, storage, and analysis. The DNA Identification Act of 1994 provided funding to law enforcement agencies for DNA collection and created the FBI's Combined DNA Index System to facilitate the sharing of DNA information among law enforcement agencies.³² Next, the Antiterrorism and Effective Death Penalty Act of 1996 authorized grants to states for developing and upgrading DNA collection procedures,³³ and the Crime Identification Technology Act of 1998 authorized additional funding for DNA analysis programs.³⁴ The resulting framework centers on the Combined DNA Index System; more than 180 law enforcement agencies throughout the country participate in the system.³⁵

In recent years, federal and state laws have expanded law enforcement authority for collecting DNA in at least two ways. First, laws have increased the range of offenses which trigger authority for collecting and analyzing DNA. In the federal context, the DNA Analysis Backlog Elimination Act of 2000 limited compulsory extraction of DNA to people who had been convicted of a "qualifying federal offense."³⁶ Under the original act, "qualifying federal offenses" included limited but selected felonies, such as murder, kidnapping, and sexual exploitation.³⁷ After September 11, 2001, the USA PATRIOT Act expanded the "qualifying federal offense" definition to include terrorism-related crimes.³⁸ In 2004, the Justice for All Act further extended the definition to reach all crimes of violence, all sexual abuse crimes, and all felonies.³⁹ Similarly, almost all states now authorize collection of DNA from people convicted of any felony.⁴⁰

Second, laws have authorized compulsory DNA collection from people who have been detained or arrested but not convicted on criminal charges. The DNA Fingerprinting Act of 2005 authorized collection "from individuals who are arrested or from non-U.S. persons who are detained under the authority of the United States."⁴¹ The Adam Walsh Child Protection and Safety Act of 2006 subsequently substituted "arrested, facing charges, or convicted" for the word "arrested" in that authority.⁴² The U.S. Department of Justice implementing regulations took effect January 9, 2009.⁴³ Mirroring the statutory language, it requires U.S. agencies to collect DNA samples from "individuals who are arrested, facing charges, or convicted, and from non-

³² P.L. 103-322, 108 Stat. 2065 (1994) (codified at 42 U.S.C. §§ 14131-14134).

³³ P.L. 104-132, 110 Stat. 1214 (1996).

³⁴ P.L. 105-251, 112 Stat. 1871 (1998).

³⁵ See FEDERAL BUREAU OF INVESTIGATION, CODIS BROCHURE, http://www.fbi.gov/about-us/lab/codis/codis_brochure.

³⁶ 42 U.S.C. § 14135a(a)(1)(B).

³⁷ P.L. 106-546, § 3, 114 Stat. 2726, 2729-30 (2000).

³⁸ P.L. 107-56, § 503, 115 Stat. 272, 364 (2001).

³⁹ P.L. 108-405, § 203(b), 118 Stat. 2260, 2270 (2004) (codified at 42 U.S.C. § 14135a(a)(2)).

⁴⁰ See NATIONAL CONFERENCE OF STATE LEGISLATURES, STATE LAWS ON DNA DATA BANKS: QUALIFYING OFFENSES, OTHERS WHO MUST PROVIDE SAMPLE (2010), available at <http://www.ncsl.org/default.aspx?tabid=12737>.

⁴¹ DNA Fingerprint Act of 2005, Tit. X, P.L. 109-162, 119 Stat. 2960. 42 U.S.C. § 14135a(a)(1).

⁴² Adam Walsh Child Protection and Safety Act of 2006, sec. 155, P.L. 109-248, 120 Stat. 587 (2006) (codified at 42 U.S.C. § 14135a(a)(1)).

⁴³ DNA-Sample Collection and Biological Evidence Preservation in the Federal Jurisdiction, 73 Fed. Reg. at 74,932, 74,935.

United States persons who are detained under authority of the United States.”⁴⁴ As mentioned, some states have likewise enacted laws authorizing collection of arrestees’ DNA.⁴⁵ Legislation was proposed in both the 111th and 112th Congress to provide incentives to encourage states to establish processes for collecting DNA from persons arrested for specified state offenses.⁴⁶

As discussed below, courts measure the intrusiveness of DNA databanking programs by considering both the circumstances under which a DNA profile was collected and the uses to which that DNA profile can be put upon its inclusion in a database. It is, therefore, noteworthy that, in addition to expanding the number and variety of circumstances under which DNA profiling is statutorily required, policymakers have expanded the number and variety of purposes for which databanked profiles can be used. In particular, the number of states that permit “familial searching” is increasing. Familial searching is a DNA database search method based on “partial matches” between the DNA profile searched and one—or several—of the DNA profiles in the database.⁴⁷ A “routine” search of a DNA database compares a complete, well-preserved DNA sample from a single source with the databanked profiles.⁴⁸ It is also a “high stringency” search, which means that it is a very discriminating search intended to produce only a “direct match.”⁴⁹ However, in some circumstances, a crime laboratory may find it necessary to conduct a lower stringency search, perhaps because the DNA sample being processed is degraded.⁵⁰ In that case, the search could generate partial matches that are less accurate than a direct match at predicting the identity of the sample’s source.⁵¹

In some states, partial matches may be recorded and used in a criminal investigation.⁵² Although some commentators characterize this method of generating partial matches as a type of familial searching, the FBI does not.⁵³ According to the FBI, familial searching entails taking a complete

⁴⁴ 28 C.F.R. § 28.12(b).

⁴⁵ See, e.g., Kan. Stat. Ann. § 21-2511(e)(2) (authorizing DNA collection from individuals arrested for any felony or certain other crimes); N.M. Stat. § 29-16-6(B) (authorizing collection of DNA samples from individuals arrested for specific violent felonies); Va. Code Ann. § 19.2-310.2:1 (requiring collection of DNA samples from “arrested for the commission or attempted commission of a violent felony”).

⁴⁶ Katie Sepich Enhanced DNA Collection Act of 2011, H.R. 988, 112th Cong. (2011); Katie Sepich Enhanced DNA Collection Act of 2011, S. 517, 112th Cong. (2011); Katie Sepich Enhanced DNA Collection Act of 2010, H.R. 4614, 111th Cong. (as passed the House, May 18, 2010). Specifically, the legislation would authorize incentive grants and bonus payments for states that institute a “minimum” or “enhanced” “DNA collection process,” respectively. A “minimum” process entails searching the federal DNA database “at least one time” against samples from individuals “arrested for or charged with” specified types of state offenses, such as those including an element of sexual contact that are punishable by at least five years imprisonment. An “enhanced” process requires the collection of samples, to be included in the federal database, from individuals “arrested for or charged with” a broader range of state law offenses, such as those with a sexual conduct element that are punishable by more than one year imprisonment. For an overview of existing federal grant programs related to the collection and law enforcement use of DNA, see CRS Report R41800, *DNA Testing in Criminal Justice: Background, Current Law, Grants, and Issues*, by Nathan James.

⁴⁷ See FEDERAL BUREAU OF INVESTIGATION, FREQUENTLY ASKED QUESTIONS (FAQS) ON THE CODIS PROGRAM AND THE NATIONAL DNA INDEX SYSTEM, <http://www.fbi.gov/about-us/lab/codis/codis-and-ndis-fact-sheet>.

⁴⁸ See *id.*; Jessica D. Gabel, *Probable Cause from Probable Bonds: A Genetic Tattle Tale Based on Familial DNA*, 21 HASTINGS WOMEN’S L. J. 3, 17-18 (2010).

⁴⁹ See FBI, *supra* note 47; Gabel, *supra* note 48, at 17.

⁵⁰ See FBI, *supra* note 47; Gabel, *supra* note 48, at 17.

⁵¹ See FBI, *supra* note 47; Gabel, *supra* note 48, at 17.

⁵² For a map of states that permit partial matching and familial searching and those that do not, see COUNCIL FOR RESPONSIBLE GENETICS, STATE RULES ON PARTIAL/FAMILIAL SEARCHING, <http://www.councilforresponsiblegenetics.org/dnadata/usa/usa2.html>.

⁵³ See FBI, *supra* note 47; Gabel, *supra* note 48, at 17. See also Natalie Ram, *DNA Confidential*, SCIENCE PROGRESS (continued...)

and well-preserved DNA sample from a single source and, usually after conducting an unsuccessful high stringency search, conducting a lower stringency search with the intent of generating partial matches.⁵⁴ In other words, under the FBI's definition, a familial search is a deliberate database search for potential *relatives* of the suspect—not for the suspect himself.⁵⁵ These searches may not be conducted in the National DNA Index System (NDIS),⁵⁶ but the FBI has developed provisional procedures for authorizing the release of inadvertently obtained partial match information to law enforcement.⁵⁷ As for state databases, some states prohibit familial searching by law⁵⁸ or by informal policy,⁵⁹ while others have permitted it.⁶⁰

Expungement Provisions

Although Congress has encouraged DNA databanking, it has also constrained the government's authority to use and retain all DNA profiles indefinitely. In particular, federal law mandates expungement of DNA samples upon an arrestee's showing of discharge or acquittal or a convict's showing that the conviction was overturned.⁶¹ These provisions apply to DNA collected by state and local law enforcement officers, in addition to DNA collected in the federal justice or detention systems. However, DNA profiles of convicts who complete their sentences are not eligible for expungement under federal law.

Expungement occurs upon written request; it does not occur automatically.⁶² To have a DNA profile expunged from the database, its source must submit, in addition to the written request, a

(...continued)

(November 2, 2009), available at <http://www.scienceprogress.org/2009/11/dna-confidential> (referring to this method as "partial match reporting" rather than "familial searching").

⁵⁴ FBI, *supra* note 47. See Gabel, *supra* note 48, at 18.

⁵⁵ See Gabel, *supra* note 48, at 18.

⁵⁶ FBI, *supra* note 47. See Gabel, *supra* note 48, at 18.

⁵⁷ FBI, *supra* note 47; U.S. Department of Justice, *Federal Bureau of Investigation Interim Plan for the Release of Information In the Event of a "Partial Match" at NDIS*, (July 20, 2006), http://www.bioforensics.com/conference08/Familial_Searches/CODIS_Bulletin.pdf.

⁵⁸ See, e.g., MD. CODE ANN., Public Safety, § 2-506(d) (prohibiting searches of the state DNA database "for the purpose of identification of an offender in connection with a crime for which the offender may be a biological relative of the individual from whom the DNA sample was acquired").

⁵⁹ According to the Council for Responsible Genetics, several states, including Alaska, Maine, Michigan, and Vermont, include prohibitions on either partial match or familial searching in lab manuals. Council for Responsible Genetics, *supra* note 52. See also Ram, *supra* note 53 (stating that research revealed that at least 12 states have unwritten policies on partial match reporting or familial searching).

⁶⁰ See, e.g., Press Release, Governor McDonnell Announces Virginia Department of Forensic Science to Begin Using Familial DNA Searches in Virginia (March 21, 2011), available at <http://www.governor.virginia.gov/News/viewRelease.cfm?id=648> (announcing that the Virginia Department of Forensic Science developed the capability to perform familial searches and issued a policy for considering requests from law enforcement officials to conduct these searches).

⁶¹ 42 U.S.C. § 14132(d).

⁶² See FEDERAL BUREAU OF INVESTIGATION, CODIS—EXPUNGEMENT POLICY, http://www.fbi.gov/about-us/lab/codis/codis_expungement. See also Sonia M. Suter, *All in the Family: Privacy and DNA Familial Searching*, 26 HARV. J. L. & TECH. 309, 341 (2010) (stating that exonerated arrestees and offenders may not be informed about the possibility of having their DNA records expunged and, even if they are, the procedures for getting the profile expunged may be overly burdensome).

certified copy of a final court order establishing that the conviction was overturned or that charges were dismissed, not filed, or resulted in acquittal.⁶³

Fourth Amendment Overview

The Fourth Amendment to the U.S. Constitution provides a right “of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.”⁶⁴ Two fundamental questions arise in every Fourth Amendment challenge. First, does the challenged action constitute a search or seizure by federal or local government and thus trigger the Fourth Amendment right?⁶⁵ Second, if so, is the search or seizure “reasonable”?

Search or Seizure

Different tests trigger the Fourth Amendment right depending on whether a litigant challenges government conduct as a seizure or as a search. Seizures involve interference with property rights; a seizure of property occurs when government action “meaningfully interferes” with possessory interests or freedom of movement.⁶⁶

In contrast, searches interfere with personal privacy. Government action constitutes a search when it intrudes upon a person’s “reasonable expectation of privacy.”⁶⁷ A reasonable expectation of privacy requires both that an “individual manifested a subjective expectation of privacy in the searched object” and that “society is willing to recognize that expectation as reasonable.”⁶⁸

In general, people have no reasonable expectation of privacy for physical characteristics they “knowingly expos[e] to the public.”⁶⁹ In evaluating whether people “knowingly expose” identifying characteristics, the Supreme Court has sometimes distinguished the drawing of blood and other internal fluids from the taking of fingerprints. At times, it has signaled that people lack a reasonable expectation of privacy in their fingerprints,⁷⁰ but it has held that extraction of blood,

⁶³ 42 U.S.C. § 14132(d). *See also* FBI, *supra* note 62 (detailing procedures for expungement).

⁶⁴ U.S. CONST. amend. IV.

⁶⁵ Courts have applied the Fourth Amendment to state and local government actions since 1961, when, in *Mapp v. Ohio*, the Supreme Court interpreted the Fourteenth Amendment as having incorporated the Fourth Amendment to the states. 367 U.S. 643, 655 (1961).

⁶⁶ *See* *United States v. Place*, 462 U.S. 696, 716 (1983) (Brennan, J., concurring in result); *Michigan v. Summers*, 452 U.S. 692, 696 (1981).

⁶⁷ Some justices and experts have noted the circularity of the combination of this definition and the general Fourth Amendment “reasonableness” inquiry. *See, e.g.*, *Minnesota v. Carter*, 525 U.S. 83, 97 (1998) (Scalia, J., concurring). However, such criticisms have not yet caused the Court to reconsider its test, except perhaps for the narrow category of interiors of homes, for which the Court has found a near-automatic reasonable expectation of privacy by virtue of privacy in the home having “roots deep in the common law.” *See* *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

⁶⁸ *Kyllo*, 533 U.S. at 33 (citing *California v. Ciraolo*, 476 U.S. 207, 211 (1986)).

⁶⁹ *Katz v. United States*, 389 U.S. 347, 351 (1967).

⁷⁰ *See, e.g.*, *Davis v. Mississippi*, 394 U.S. 721, 727 (1969) (“Fingerprinting involves none of the probing into an individual’s private life and thoughts that marks an interrogation or search.”). Later, in *Hayes v. Florida*, the Supreme Court seemed to suggest that fingerprinting does constitute a search, 470 U.S. 811, 814 (1985) (referring to fingerprinting as less intrusive than *other* types of searches and seizures), a shift in keeping with the Court’s broader trend toward classifying more activity as constituting a search and leaving the heart of the constitutional analysis for the Fourth Amendment “reasonableness” inquiry. Thus, it appears that although the Court views the drawing of blood as a (continued...)

urine, and other fluids implicates an intrusion upon a reasonable expectation of privacy, presumably because the former category is “knowingly exposed” to the public while the latter category generally is not.⁷¹

Under modern Supreme Court precedent, a further complicating factor is that reasonable expectation of privacy depends not only on the type of evidence gathered, but also on the status of the person from whom it is gathered. The inquiry is not simply a yes-or-no determination, but appears to include a continuum of privacy expectations. For example, in *United States v. Knights*,⁷² the Court held that the “condition” of probation “significantly diminished” a probationer’s reasonable expectation of privacy.⁷³ This diminished privacy expectation did not completely negate the probationer’s Fourth Amendment right; however, it affected the outcome under the Court’s Fourth Amendment balancing test.⁷⁴

“Reasonableness” Inquiry When the Fourth Amendment Applies

When government action constitutes a search or seizure, “reasonableness” is the “touchstone” of constitutionality.⁷⁵ However, courts apply different standards, in different circumstances, to determine whether searches and seizures are reasonable.⁷⁶ In general, courts have measured the Fourth Amendment consistency of DNA databanking programs under the “general balancing” test—also called the “general reasonableness,” or “totality-of-the-circumstances” test. Used to assess the constitutionality of “administrative,” “special needs,” and other “suspicionless” searches, such as roadblocks and drug testing, this analysis weighs the “degree to which [a search or seizure] intrudes upon an individual’s privacy” with “the degree to which it is needed for the promotion of legitimate governmental interests.”⁷⁷

(...continued)

greater intrusion than fingerprinting, both activities now qualify as searches.

⁷¹ See, e.g., *Skinner v. Ry. Labor Executives’ Ass’n*, 489 U.S. 602, 616 (1989) (“We have long recognized that a ‘compelled intrusio[n] into the body for blood to be analyzed for alcohol content’ must be deemed a Fourth Amendment search” (quoting *Schmerber v. California*, 384 U.S. 757, 767-768 (1966)). This distinction contrasts with the Supreme Court’s rejection of a blood-versus-fingerprints distinction in the context of the confrontation clause to the Sixth Amendment of the U.S. Constitution, wherein the Court has held neither fingerprinting nor the taking of blood are barred because they are both “real and physical” rather than “testimonial” evidence. See *Pennsylvania v. Muniz*, 496 U.S. 582, 591 (1990).

⁷² 534 U.S. 112 (2001).

⁷³ *Id.* at 119-120.

⁷⁴ *Id.*

⁷⁵ *Id.* at 118.

⁷⁶ There are three general categories of Fourth Amendment analysis. The first category involves traditional law enforcement activities, such as arrests or searching of homes. To be reasonable, these activities require “probable cause,” which must be formalized by a warrant unless a recognized warrant exception applies. *Atwater v. City of Lago Vista*, 532 U.S. 318, 354 (2001). This is considered the most stringent Fourth Amendment standard. The second category involves situations in which a limited intrusion, such as a pat-down, satisfies Fourth Amendment strictures if the search was justified by “reasonable suspicion” based on “specific reasonable inferences.” *Alabama v. White*, 496 U.S. 325, 330 (1990); *Terry v. Ohio*, 392 U.S. 1, 21-22, 27 (1968). Courts apply the third test, the “general balancing” test, to assess “exempted area,” “administrative,” “special needs,” and other “suspicionless” searches. *Samson v. California*, 547 U.S. 843, 848 (2006).

⁷⁷ *Samson*, 547 U.S. at 848.

Historically, courts used the general reasonableness test only in three situations: (1) when a routine, administrative purpose justified regular searches; (2) where a long-recognized warrant exception existed, such as for border searches; and (3) where a “special need, beyond the normal need for law enforcement, [made] the warrant and probable cause requirements impracticable.”⁷⁸ Recently, however, the Supreme Court has supplied a new justification for applying this test: the person’s status within the penal system.⁷⁹

Noting that parolees must comply with certain rules and conditions imposed by the government, the Supreme Court has held that a person’s status as a parolee entitles the courts to evaluate a potentially unconstitutional search of that person under the general reasonableness test.⁸⁰ Federal courts now place the privacy rights of prisoners, parolees, probationers, and supervised releasees on a spectrum, describing each category as having slightly greater privacy rights than the one preceding it.⁸¹

Collecting DNA

The Supreme Court has not accepted a case reviewing a compulsory DNA collection statute. However, the courts have uniformly held that compulsory DNA collection and analysis constitutes a search, and thus triggers Fourth Amendment rights.⁸² Accordingly, compulsory DNA collection and profiling laws violate the Fourth Amendment if they fail the reasonableness test. The reasonableness analysis varies, however, with the degree to which the law enforcement system has authority over the subject at the time of the search.⁸³ Therefore, a court’s analytical

⁷⁸ *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1986) (citing *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring)).

⁷⁹ *See, e.g., Samson v. California*, 547 U.S. 843, 848-850 (2006) (upholding a search of a parolee’s pockets, for the first time directly applying the general reasonableness test to a search justified only on the basis of the petitioner’s status as a parolee, rather than on any particularized suspicion). *United States v. Knights*, 534 U.S. 112, 114-120 (2001) (evaluating a warrantless search of a probationer’s home under the general reasonableness test because the conditions placed on his probation significantly diminished the reasonableness of his expectation of privacy). *See also Griffin v. Wisconsin*, 483 U.S. 868, 873-74 (1986) (applying the general reasonableness test to a search of a person’s home because the person was on probation). Some courts have characterized this new basis for the general reasonableness test as one of the long-recognized warrant exceptions. *See, e.g., United States v. Pool*, 621 F.3d 1213, 1218 (9th Cir. 2010).

⁸⁰ *Samson*, 547 U.S. at 848-852.

⁸¹ *See, e.g., Wilson v. Collins*, 517 F.3d 421, 425 n.2, 426-27 (6th Cir. 2008) (describing a “privacy continuum” on which “a parolee ... has less diminished privacy rights than a prisoner”). Parole and supervised release are sometimes conflated, but they represent two distinct forms of post-incarceration supervision by the state. *See UNITED STATES SENTENCING COMMISSION, 2010 FEDERAL SENTENCING GUIDELINES MANUAL 484* (2010), available at http://www.ussc.gov/Guidelines/2010_guidelines/ToC_PDF.cfm. Whereas parolees are on release from incarceration *before* the end of their sentence, supervised releasees are serving a term of state supervision *after* their initial term of incarceration. *See id.*

⁸² *See, e.g., United States v. Amerson*, 483 F.3d 73, 77 (2d Cir. 2007), cert. denied 552 U.S. 1042 (2007) (“It is settled law that DNA indexing statutes, because they authorize both a physical intrusion to obtain a tissue sample and a chemical analysis to obtain private physiological information about a person, are subject to the strictures of the Fourth Amendment.”).

⁸³ *See Wilson v. Collins*, 517 F.3d 421, 426-27 (6th Cir. 2008). *See also United States v. Kriesel*, 508 F.3d 941, 948-49 (9th Cir. 2007) (“We emphasize that our ruling today does not cover DNA collection from arrestees or non-citizens detained in the custody of the United States, who are required to submit to DNA collection by the 2006 version of the DNA Act”).

approach toward collecting DNA from a convicted criminal may differ—and yield a different outcome—than its approach toward collecting DNA collection from an arrestee.

Prisoners, Parolees, Probationers, and Supervised Releasees

On the “privacy continuum” prisoners, parolees, probationers, and supervised releasees share diminished, but not necessarily equivalent, privacy rights.⁸⁴ Moreover, according to the federal appeals courts, the privacy rights of all four types of convicted offenders are diminished to such an extent that they have no reasonable expectation of privacy in their DNA or DNA profile.⁸⁵ Indeed, the vast majority of U.S. Courts of Appeals have upheld either the federal law mandating DNA collection and analysis from prisoners, parolees, and probationers or a similar state law.⁸⁶

In these cases, the only source of conflict between the courts appears to be the appropriate rationale for evaluating these laws under the general reasonableness test.⁸⁷ A majority of courts use the state’s court-ordered supervision of the subject as their sole rationale for applying the general reasonableness test.⁸⁸ However, some federal circuit courts of appeals continue to apply the traditional special needs methodology, assessing whether the collection of the subject’s DNA was justified by a “special need beyond the ordinary needs of normal law enforcement” before evaluating whether the government’s acquisition and use of the subject’s DNA was reasonable.⁸⁹ Although courts have noted this analytical distinction, it may have no practical import because, regardless of the standard applied, courts have consistently upheld compulsory post-conviction DNA collection laws.⁹⁰

⁸⁴ See *Wilson*, 517 F.3d at 425 n.2.

⁸⁵ See, e.g., *United States v. Weikert*, 504 F.3d 1, 3 (1st Cir. 2007) (upholding provision of the federal law mandating DNA collection from a supervised releasee); *United States v. Amerson*, 483 F.3d 73, 89 (2d Cir. 2007) (upholding provisions of the federal law mandating DNA collection from a probationer); *Wilson*, 517 F.3d at 423 (upholding a state law mandating DNA collection from a prisoner).

⁸⁶ E.g., *Weikert*, 504 F.3d at 3 (holding for the First Circuit that the federal law is consistent with the U.S. Constitution); *Amerson*, 483 F.3d at 89 (upholding the federal law), *cert. denied* 552 U.S. 1042 (2007); *United States v. Hook*, 471 F.3d 766 (7th Cir. 2006) (upholding the federal law), *cert. denied* 549 U.S. 1343 (2007); *United States v. Kraklio*, 451 F.3d 922 (8th Cir. 2006) (upholding the federal law), *cert. denied* 549 U.S. 1044 (2006); *Kriesel*, 508 F.3d at 942 (upholding the federal law); *United States v. Banks*, 490 F.3d 1178 (10th Cir. 2007) (upholding the federal law); *United States v. Castillo-Lagos*, 147 Fed. App’x. 71 (11th Cir. 2005) (upholding the federal law); *Jones v. Murray*, 962 F.2d 302 (4th Cir. 1992) (upholding the Virginia statute). See also *Padgett v. Donald*, 401 F.3d 1273 (11th Cir. 2005) (upholding the Georgia statute); *Green v. Berge*, 354 F.3d 675 (7th Cir. 2004) (upholding the Wisconsin statute); *Shaffer v. Saffle*, 148 F.3d 1180 (10th Cir. 1998) (upholding the Oklahoma statute); *Schlicher v. Peters*, 103 F.3d 940 (10th Cir. 1996) (upholding the Kansas statute); *Boling v. Romer*, 101 F.3d 1336 (10th Cir. 1996) (upholding the Colorado statute).

⁸⁷ See *Amerson*, 483 F.3d at 78 (stating that the courts have nearly unanimously upheld state and federal DNA databanking laws, but, in doing so, have used two different approaches); *Kraklio*, 451 F.3d at 924 (“The only disagreement among the circuits is what analytical approach to use in upholding the [DNA collection] statutes.”); *United States v. Kincade*, 379 F.3d 813, 830-31 (9th Cir. 2004) (“Confronted with challenges to the federal DNA Act and its state law analogues, our sister circuits and peers in the states have divided in their analytical approaches” between a traditional special needs analysis and a direct assessment of reasonableness).

⁸⁸ See, e.g., *Wilson*, 517 F.3d at 426 (finding that the direct application of the general balancing test is appropriate in a case involving a prisoner). See also *Amerson*, 483 F.3d at 78 (describing the Second Circuit’s insistence on the traditional special needs test methodology as in conflict with the Third, Fourth, Fifth, Ninth, and Eleventh Circuits).

⁸⁹ See, e.g., *Amerson*, 483 F.3d at 78-80 (articulating the traditional methodology of a special needs test, justifying its application to compulsory DNA collection laws, and applying it).

⁹⁰ See, e.g., *Wilson*, 517 F.3d at 427 n. 4 (“Even if we were to apply the more stringent special-needs test, there is no reason to believe the ultimate result would be different.”).

Arrestees

The statutory authorization of compulsory DNA collection from arrestees appears to have constitutionally significant implications for DNA databanking programs. Congress's apparent goal in requiring the databanking of arrestees' DNA was to facilitate crime prevention through "the creation of a comprehensive, robust database that will make it possible to catch serial rapists and murderers before they commit more crimes."⁹¹ However, the handful of state⁹² and federal⁹³ judicial decisions to address compulsory collection of DNA from persons awaiting a criminal trial show that the courts are split over the constitutionality of this policy.

In *United States v. Pool*,⁹⁴ the Ninth Circuit Court of Appeals affirmed a lower court's ruling that conditioning an arrestee's pre-trial release on DNA sampling is consistent with the Fourth Amendment. However, in *United States v. Mitchell*,⁹⁵ the U.S. District Court for the Western District of Pennsylvania reached the opposite result. An appeal is now pending before the Third Circuit Court of Appeals.

In both cases, the government requested a DNA sample after the defendant's arrest and criminal indictment but before trial.⁹⁶ The courts agreed that the direct application of the general reasonableness test was appropriate, characterizing the judicial or grand jury finding of probable

⁹¹ 151 CONG. REC. S13756 (daily ed. December 16, 2005) (statement of Sen. Kyl). In background material for its implementing rule, the Justice Department explains that collection from arrestees will facilitate more effective law enforcement for at least two reasons: (1) it will aid in crime prevention by ensuring that the government need not wait until a crime has been committed before creating an individual's DNA profile; and (2) it will allow federal authorities to create DNA profiles for aliens detained in the United States, who might not otherwise undergo judicial proceedings in U.S. courts. DNA-Sample Collection and Biological Evidence Preservation in the Federal Jurisdiction, 73 Fed. Reg. at 74,934.

⁹² This report focuses on federal court decisions, but several state courts have also reviewed the collection of DNA from arrestees, with mixed results. For example, the Virginia Supreme Court upheld Virginia's statute authorizing DNA collection from arrestees. *Anderson v. Virginia*, 650 S.E.2d 702 (Vir. 2006), *cert. denied*, 553 U.S. 1054 (2008). In contrast, the Minnesota Court of Appeals held that a state law authorizing collection of a DNA sample "upon a finding of probable cause, but before any conviction ..." violated the Fourth Amendment to the U.S. Constitution and Article 1, Section 10 of the Minnesota Constitution. In the Matter of the Welfare of C.T.L., 722 N.W.2d 484, 486 (Minn. Ct. App. 2006).

⁹³ In addition to the two federal district court cases discussed in this report, two other federal judicial decisions, both issued in December 2009, are of interest. First, in *Friedman v. Boucher*, the U.S. Court of Appeals for the Ninth Circuit denied Nevada police officers' motion for qualified immunity where the officers, acting on their own volition rather than pursuant to any state or federal law, forced the collection of DNA from a man in pre-trial detention for the purpose of comparing his DNA to evidence available in "cold cases." 580 F.3d 847 (9th Cir. 2009). The Ninth Circuit emphasized the lack of statutory authority and the absence of a strong governmental interest in the case. Given those fact-specific underpinnings for its decision, it is unclear whether the Ninth Circuit's rationale would apply in a future case in which statutory authority and a different governmental interest existed. Second, in *Haskell v. Brown*, the U.S. District Court for the Northern District of California denied a motion to enjoin the enforcement of a California statute requiring the collection of DNA from adults arrested for felony offenses. 677 F. Supp. 2d 1187 (N.D.Cal. 2009). Because the case arose at the preliminary injunction stage, it is unclear how much weight the decision might have on a future challenge to California's law.

⁹⁴ 645 F. Supp.2d 903 (E.D. Cal. 2009), *aff'd*, *United States v. Pool*, 621 F.3d 1213 (9th Cir. 2010).

⁹⁵ 681 F.Supp.2d 597 (W.D.Pa. 2009), *appeal docketed*, *United States v. Mitchell*, No. 09-4718 (3d Cir. 2011). Oral arguments in the appeal can be heard at <http://www.ca3.uscourts.gov/oralargument/ListArgumentsAll.aspx>.

⁹⁶ In *Pool*, the defendant was granted pre-trial release. For that reason, a provision of the Bail Reform Act, 18 U.S.C. § 3142(b), which requires DNA collection as a condition of pre-trial release, provided a supplementary basis of statutory authority.

cause for an arrest as a “watershed event” after which the arrestees’ privacy rights were so diminished as to make some warrantless and suspicionless searches reasonable.⁹⁷

Given that the courts in *Pool* and *Mitchell* applied the same analytical approach, the divergence in their outcomes arose not from dissimilar legal standards so much as conflicting interpretations of the facts. Namely, the courts adopted strikingly different views of the extent to which (1) the arrestee’s privacy rights were diminished upon the probable cause determination; (2) DNA collection and databanking intruded upon a person’s privacy interests; and (3) DNA profiling served a substantial government interest.

As to the diminishment of the arrestee’s privacy rights, the Ninth Circuit affirmed the lower court’s view that these rights are substantially diminished by the arrestee’s indictment.⁹⁸ For support, the Ninth Circuit pointed to other legitimate ways that the state may exercise control over an indicted arrestee such as electronic monitoring and mandatory curfews.⁹⁹ However, the *Mitchell* court criticized this approach as inconsistent with “the moral polestar” of the U.S. criminal justice system: the presumption of innocence.¹⁰⁰ The *Mitchell* court wrote that, because the state must meet a higher standard of proof than probable cause to prove an arrestee’s guilt, the arrestee’s privacy rights are diminished only to the extent necessitated by “legitimate penological interests,” such as prison security.¹⁰¹ According to the *Mitchell* court, an arrestee maintains an *undiminished* expectation of privacy in his genetic code.¹⁰²

On the extent of the privacy intrusion, *Pool* characterized DNA profiling as no more intrusive than fingerprinting or photographing a suspect.¹⁰³ The court in *Mitchell*, on the other hand, rejected this analogy on the basis of genetic exceptionalism.¹⁰⁴ Noting that the arrestee’s DNA sample, even if not the resulting profile, would contain information about his predisposition to genetic conditions and, perhaps, behavioral traits, the court characterized DNA collection as an act of “information science”—a “quantum leap” in terms of intrusiveness from the “*identification science*” involved in fingerprinting.¹⁰⁵

Finally, the courts characterized the government’s interests—and their importance—differently. In *Pool*, the Ninth Circuit listed numerous “substantial” governmental interests in DNA databanking, including (1) determining whether the individual may be released pending trial without endangering society; (2) discouraging the individual from violating the conditions of pre-trial release; (3) ensuring that the defendant did not commit some other crime; and (4) knowing

⁹⁷ *Pool*, 621 F.3d at 1218-19. See *Mitchell*, 681 F.Supp.2d at 604-05 (writing that although it disagrees with the holding in *Pool*, it agrees with the analysis in *Pool* of an arrestee’s status for the purpose of determining the applicability of the special needs test).

⁹⁸ See *Pool*, 621 F.3d at 1219.

⁹⁹ *Id.*

¹⁰⁰ *Mitchell*, 681 F. Supp. at 606.

¹⁰¹ *Id.* at 606-07.

¹⁰² *Id.* at 608.

¹⁰³ *Pool*, 621 F.3d at 1221-22. See also *Pool*, 645 F. Supp.2d at 911 (“The court agrees that DNA sampling is analogous to taking fingerprints ...”).

¹⁰⁴ See *Mitchell*, 681 F.Supp.2d at 608. The court described the contention that DNA is analogous to fingerprints as “pure folly.” *Id.*

¹⁰⁵ *Id.* at 609 (emphasis added).

who is being released to the public.¹⁰⁶ In contrast, the court in *Mitchell* described the government's sole interest in collecting DNA as suspect identification, a "legitimate" but not "compelling" objective that could be achieved through fingerprinting and photographing—methods it deemed less intrusive than DNA profiling.¹⁰⁷

Using and Retaining Databanked DNA

In addition to the constitutionality of compulsory DNA collection, a second set of emerging Fourth Amendment issues with DNA database programs concerns the retention and use of DNA samples and profiles. As mentioned, federal law requires the FBI to expunge DNA profiles for people who receive acquittals or whose convictions are overturned.¹⁰⁸ Courts have pointed to these provisions as reducing the intrusiveness of collecting DNA samples from arrestees.¹⁰⁹ This case law suggests that sources of lawfully collected and databanked DNA maintain some degree of privacy interests in their DNA profiles. However, it is not clear whether *convicted* felons retain those rights as well, and, if they do, what types of actions would unreasonably intrude upon those rights.

Post-Sentence Privacy Rights

The federal expungement provisions do not address storage of DNA from people who have successfully completed their sentences. Rather, once a person's DNA profile has been entered into CODIS database, "police at any level of government with a general criminal investigative interest ... can tap into that DNA without any consent, suspicion, or warrant, long after his period of supervised release ends."¹¹⁰ Convicted felons who have completed their sentences have initiated Fourth Amendment challenges to the government's indefinite storage of their DNA profiles and samples.¹¹¹ However, few courts have been convinced by their arguments. In particular, judicial skepticism of genetic exceptionalism has made it difficult for defendants to overcome the established constitutionality of the government's indefinite retention of fingerprints and other identification records of convicted felons.¹¹²

¹⁰⁶ *Pool*, 621 F.3d at 1223.

¹⁰⁷ *Mitchell*, 681 F.Supp.2d at 609.

¹⁰⁸ 42 U.S.C. § 14132(d).

¹⁰⁹ *See, e.g., Pool*, 621 F.3d at 1227 n.16 ("The alleged intrusion on any of Pool's rights is also reduced by the provision that the DNA sample may be expunged if he is not found guilty or his case is dismissed.")

¹¹⁰ *United States v. Kriesel*, 508 F.3d 941, 952 (9th Cir. 2007).

¹¹¹ *See, e.g., Boroian v. Mueller*, 616 F.3d 60, 68 n.6 (1st Cir. 2010); *United States v. Amerson*, 483 F.3d 73 (2d Cir. 2007); *Johnson v. Quander*, 440 F.3d 489, 499 (D.C. Cir. 2006).

¹¹² *See, e.g., Boroian*, 616 F.3d at 67 ("[I]dentification records of convicted felons, such as fingerprints or mugshots, are routinely retained by the government after their sentences are complete and may be expunged only in narrowly defined circumstances ... [P]recedents hold that the government's matching of a lawfully obtained identification record against other records in its lawful possession does not infringe on an individual's legitimate expectation of privacy"); *United States v. Amerson*, 483 F.3d 73, 86 (2d Cir. 2007) ("[I]t is well established that the state need not destroy records of identification—such as fingerprints, photographs, etc.—of convicted felons, once their sentences are up. The same applies to DNA"); *Johnson v. Quander*, 440 F.3d 489, 499 (D.C. Cir. 2006) ("Police departments across the country could face an intolerable burden if every 'search' of an ordinary fingerprint database were subject to Fourth Amendment challenges. The same applies to DNA fingerprints ... CODIS operates much like an old-fashioned fingerprint database (albeit more efficiently)"). *See also Stevenson v. United States*, 380 F.2d 590 (D.C. Cir.), *cert. denied*, 389 U.S. 962 (1967) (holding that a defendant had no constitutional right to the expungement of his mugshots (continued...))

Nevertheless, like the cases over DNA collection from an arrestee, cases upholding the government's use and storage of databanked DNA after its source completes his sentence illustrate diverging views of the information collected through DNA database programs. In particular, dicta in state and federal court opinions augur judicial divergence over the extent to which an offender retains privacy rights in his DNA sample and profile after his full release from the penal system.

The First Circuit acknowledged this apparent dissensus in its 2010 case, *Boroian v. Mueller*.¹¹³ In that case, the court upheld the government's indefinite retention and periodic matching of a felon's DNA after his sentence was completed.¹¹⁴ However, it also expressly refused to hold "as some courts have suggested" that, upon a DNA sample's lawful extraction and databanking, its source "loses a reasonable expectation of privacy with respect to *any* subsequent use of that profile."¹¹⁵ Instead, the First Circuit ruled that, once a qualified offender's DNA "profile has been lawfully created and entered into CODIS ... the FBI's retention and periodic matching of the profile against other profiles in CODIS for the purpose of *identification* is not an intrusion on the offender's legitimate expectation of privacy."¹¹⁶ In other words, *Boroian* suggests that there could be circumstances in which the post-sentence retention and use of a DNA profile violate its source's reasonable expectation of privacy.

As the First Circuit in *Boroian* pointed out, however, several state courts have not reached such a limited conclusion,¹¹⁷ and their more expansive view may have support within the federal judiciary. For example, the Supreme Court of the State of Hawaii held in *State v. Hauge*¹¹⁸ that "once a blood sample and DNA profile is lawfully procured from a defendant, *no* privacy interest ... in either the sample or the profile" prevents its indefinite use and retention by the government.¹¹⁹ Significantly, Judge Easterbrook of the U.S. Court of Appeals for the Seventh Circuit expressed support for this perspective in his concurrence in the 2004 case *Green v. Berge*,¹²⁰ in which he wrote that lawfully obtained DNA samples may be put to a wide variety of uses beyond indefinite storage and periodic matching because "the Fourth Amendment does not control how properly collected information is deployed."¹²¹

(...continued)

and fingerprints after his conviction was set aside).

¹¹³ 616 F.3d 60 (1st Cir. 2010).

¹¹⁴ *Id.* at 68.

¹¹⁵ *Id.* (emphasis in original).

¹¹⁶ *Id.*

¹¹⁷ *Id.* See also *State v. Hauge*, 79 P.3d 131, 144 (Haw. 2003) (holding that the defendant had no reasonable privacy interest in his DNA sample or profile after it had been lawfully collected); *Patterson v. State*, 742 N.E.2d 4, 16-17 (Ind. Ct. App. 2000) ("[S]ociety is not prepared to recognize as reasonable [the defendant's] continued expectation of privacy in blood samples *lawfully* collected by police" (emphasis in original)).

¹¹⁸ 79 P.3d 131 (Haw. 2003)

¹¹⁹ *Id.* at 144 (Haw. 2003) (emphasis added).

¹²⁰ 354 F.3d 675 (7th Cir. 2004) (Easterbrook, J., concurring).

¹²¹ *Id.* at 680.

Informational Privacy Rights

The difference between the First Circuit's view in *Boroian* and Judge Easterbrook's opinion in *Green* has significant implications for the potential uses of DNA databases and the information they contain. Database opponents characterize laws that authorize or condone the use of DNA databases to research anything other than a suspect's identity as making the database program particularly intrusive.¹²² Although these concerns have yet to form the basis of a Fourth Amendment challenge to a DNA databanking program, they are premised on a belief that people retain a substantial privacy interest in the information encoded in their DNA even after they have been convicted and their DNA lawfully included in a DNA database.

Academic Research and Non-forensic Information

Congress has generally sought to restrict the non-forensic use of DNA databases to those with the potential to enhance the forensic utility of CODIS.¹²³ The DNA Analysis Backlog Elimination Act of 2000 criminalized both (1) the knowing disclosure of a sample or DNA analysis to someone who is not authorized to receive it and (2) the unauthorized acquisition or use of such a sample or analysis.¹²⁴ However, federal law does not also entitle individuals aggrieved by the misuse of their profiles to pursue a private cause of action against those responsible.¹²⁵ In other words, federal law prohibits most non-forensic uses of DNA databases but does not authorize private individuals to enforce this prohibition.

While database opponents would like to see federal law incorporate a private cause of action, their primary concern is with state laws that permit a wider range of non-forensic uses of state DNA databases. Some state legislatures, for example, have expressly authorized the use of the state DNA database for medical and academic research.¹²⁶ In the eyes of database opponents,

¹²² See, e.g., Sonia M. Suter, *supra* note 62, at 335 (contending that familial searching could unlawfully invade the privacy of the "offender or arrestee, his family members, and the family itself" and expressing concern over the possibility that, in some states, a DNA database could be used to conduct research on its sources' traits and diseases); Gabel, *supra* note 48, at 4-5 (arguing that cases involving familial DNA searches "raise legitimate concerns about the rise of the silent informant" and "represent a troubling addition to the increasing collection, retention, and use of genetic information"). See also Memorandum from Seth Axelrad for The American Society of Law, Medicine and Ethics (ASLME), available at http://www.aslme.org/dna_04/reports/axelrad3.pdf (describing different state policies toward the non-forensic use of DNA databases).

¹²³ See 42 U.S.C. § 14132(b)(3) (authorizing the use of DNA profiles in CODIS for forensic identification purposes, related legal proceedings, and, once personally identifiable information is removed, a "population statistics database"). See also D.H. Kaye, *Behavioral Genetics and Criminal DNA Databases*, 69 LAW & CONTEMP. PROBS. 259, 276 (2006) (explaining how population statistics databases, protocol development, and quality control research all fit within the "identification paradigm").

¹²⁴ P.L. 106-546, § 3(a)(5), codified at 42 U.S.C. § 14135e(c).

¹²⁵ Compare e.g., *id.* (making the knowing or intentional disclosure or use of a confidential DNA forensic record or analysis a felony but not establishing a private cause of action for the aggrieved individual) with RIGEN. LAWS § 12-1.5-15 (criminalizing violations of the confidentiality conditions on the use of DNA samples and authorizing a person aggrieved by a violation to bring a civil action for damages, injunctive relief, and attorneys' fees) and VT. STAT. ANN. tit. 20, § 1941 (criminalizing violations of the confidentiality conditions on the use of DNA samples and authorizing a person aggrieved by a violation to pursue a private action for all "appropriate relief").

¹²⁶ See, e.g., MICH. COMP. LAWS § 28.176(2)(d) (permitting DNA profiles contained in the database to be used, *inter alia*, for an "academic," "research," or "statistical" analysis if "personal identifications" are removed); Ala. Code § 36-18-31 (authorizing the creation of a "DNA population statistical database" that may be used to, *inter alia*, "provide data relative to ... disease or disability" and "assist in other humanitarian endeavors including, but not limited to, educational research or medical research or development"). See also ARK. CODE ANN. § 12-12-1018(d) (authorizing the creation of (continued...))

these states have established databanking programs that are more intrusive for the purposes of the Fourth Amendment than those that follow the stricter federal standards.¹²⁷

Although these claims have not been raised before a federal judge, they can draw support from language in existing case law. Several courts have considered, as part of their Fourth Amendment analysis, both the range of purposes for which a given DNA database can be used and the penalties for any misuse.¹²⁸ However, courts have also indicated that, until a case presents facts establishing that a DNA database was used for a non-forensic purpose, a court cannot accurately measure any resulting privacy intrusion or assess its Fourth Amendment reasonableness.¹²⁹

Familial Searching and Information About Genetic Relationships

Although concerns about possible non-forensic use of DNA databases are reflected in state and federal laws, the universe of possible *forensic* uses of DNA databases has generated greater public concern in recent years. In particular, the technique known as “familial searching” has received widespread media attention—both positive and negative—over the last decade.¹³⁰

As discussed above, the FBI defines a familial search as a deliberate database search for potential *relatives* of the suspect. Federal courts have not yet had an occasion to assess the constitutionality of familial searching. Some of the privacy interests implicated by familial searching are different from those implicated by more routine DNA database searches.¹³¹ In particular, commentators have asserted that familial searching may violate two types—and more than one person’s—privacy interests.¹³² The first type is the privacy interests of the person whose DNA profile was located as a partial match. Commentators assert that this person has a privacy interest in information about his genetic relationships, information that may be revealed by a familial search of the DNA database.¹³³ The second set of privacy interests belongs to family members of the

(...continued)

a “population database” composed of DNA samples stored in the database with the “personal identification” removed).

¹²⁷ See, e.g., Suter, *supra* note 62, at 335, 338 (stating that “vague legislative limits on the uses of the samples” risk, if not empower, government searches that exceed their legal boundaries and raise “civil liberty concerns by increasing the extent and breadth of government intrusions”). *But see* Kaye, *supra* note 123, at 260 (rejecting some of the theories, both legal and scientific, that underpin this argument). Database opponents are also concerned that not all states have expressly prohibited using DNA databases—and the information contained therein—for non-forensic research. See, e.g., Suter, *supra* note 62, at 336 (stating that there are 40 jurisdictions that neither authorize nor prohibit non-forensic uses and, in those states, there is “uncertainty as to the legal limits” on the uses of stored samples). For example, Idaho lists permissible uses of collected DNA samples and profiles but does not expressly prohibit potential non-forensic uses. IDAHO CODE ANN. §§ 19-5505, 19-5514.

¹²⁸ See, e.g., *Banks v. United States*, 490 F.3d 1178, 1192, 1193 (10th Cir. 2007) (weighing “the plaintiffs’ diminished privacy rights, the minimal intrusion involved in obtaining a DNA sample, and the Act’s restrictive provisions” against the governmental interests (emphasis added)); *United States v. Amerson*, 483 F.3d 73, 85 (2d Cir. 2007) (finding that the privacy invasion occasioned by the maintenance of DNA profiles is minimal because, *inter alia*, “the Act severely limits the circumstances and purposes for which the DNA profiles can be released”).

¹²⁹ See *Amerson*, 483 F.3d at 87; *United States v. Kincade*, 379 F.3d 813, 837-38 (9th Cir. 2004).

¹³⁰ See, e.g., Maura Dolan, *State to Double Crime Searches Using Family DNA*, L.A. TIMES (May 9, 2011); Jessica Cerretani, *Whodunit? BOSTON GLOBE* (October 31, 2010); Natasha Singer, *In Fighting Crime, How Far Should a Genetic Net Reach? N.Y. TIMES* (July 24, 2010); Jeffrey Rosen, *Genetic Surveillance for All*, SLATE (March 17, 2009), <http://www.slate.com/id/2213958>.

¹³¹ See, e.g., Suter, *supra* note 62, at 327-28.

¹³² See, e.g., *id.* at 342.

¹³³ See, e.g., *id.* at 342, 343.

person whose profile was a partial match. Law enforcement may violate these privacy rights if, while following up on the lead provided by the partial match, they collect DNA from the partial match's family members without a warrant.¹³⁴ These family members may have privacy interests in their genetic identities as well as in their genetic relationship—or lack thereof—with the person who claimed they were kin.

Because the constitutionality of familial searching has not yet reached the federal courts, the existence of a reasonable privacy interest in genetic relationships remain a largely untested assertion. Commentators defend its existence on the grounds that, unlike other types of information, people do not knowingly expose their genetic relationships and, moreover, may not necessarily be credited with knowledge—let alone amenability to public exposure—of their genetic kin.¹³⁵

Implications of New Research on Junk DNA

Despite the “rapid pace of technological development in the area of DNA analysis,”¹³⁶ much of DNA's scientific value remains a mystery. As mentioned, FBI analysts rely on junk DNA precisely because it is not believed to reveal sensitive medical or biological information. Partly for that reason, proponents of expansive DNA collection argue that any privacy intrusion resulting from DNA storage or analysis is minimal at most. For example, when he introduced the amendment that authorizes collection and analysis of DNA from arrestees in the federal system, Senator Kyl emphasized that storage of DNA samples would not intrude upon individuals' privacy rights, stating that “the sample of DNA that is kept ... is what is called ‘junk DNA’—it is impossible to determine anything medically sensitive from this DNA.”¹³⁷ Likewise, courts have assumed that DNA analysis and storage involves only a minimal privacy intrusion.

However, language in some opinions suggests that this assumption might change if scientists discover new uses for junk DNA. Both the First Circuit and the Second Circuit have suggested that “discovery of new uses for ‘junk DNA’ would require a reevaluation of the [Fourth Amendment] reasonableness balance.”¹³⁸ In addition, at least two judges on the Ninth Circuit

¹³⁴ See, e.g., *State v. Athan*, 158 P.3d 27, 33-34 (Wash. 2007) (considering—and upholding—the constitutionality of collecting DNA by posing a fictitious law firm, inviting the suspect to join a class action lawsuit via mail, and collecting his saliva from the sealed return envelope). See also, Suter, *supra* note 62, at 358 (suggesting that a partial match alone cannot satisfy the probable cause test because current forensic testing does not establish a sufficiently high probability of a biological connection between the source of the partial match and the suspect).

¹³⁵ See, e.g., Suter, *supra* note 62, at 364 (listing circumstances in which the source of the databanked profile with similarities to the suspect's may be unaware that he had a sibling who was given up for adoption or that one of his children is the product of his partner's adultery).

¹³⁶ *United States v. Weikert*, 504 F.3d 1, 3 (1st Cir. 2007).

¹³⁷ 151 CONG. REC. S13757 (daily ed. December 16, 2005) (statement of Sen. Kyl).

¹³⁸ *United States v. Stewart*, 532 F.3d 32, 36 (1st Cir. 2008); *United States v. Amerson*, 483 F.3d 73, 85 n.13 (2d Cir. 2007) (“Should the uses to which ‘junk DNA’ can be put be shown in the future to be significantly greater than the record before us today suggests, a reconsideration of the reasonableness balance would be necessary”). See also *Haskell v. Brown*, 677 F. Supp. 2d 1187, 1190 n.1 (N.D. Cal. 2009) (noting that “so-called ‘junk’ DNA might someday be found to contain genetic programming material,” but stating that the court's opinion must be based on “the facts as they are ... today.”).

have expressed concern about the potential for profiles developed from junk DNA to yield more sensitive information about their sources in the future.¹³⁹

Scientific research on junk DNA is still emerging, and some research suggests that junk DNA contains more genetic information than previously assumed. For example, in October 2008, University of Iowa researchers released study findings showing that junk DNA has the potential to “evolve into exons, which are the building blocks for protein-coding genes.”¹⁴⁰ Other scientists have similarly hypothesized that there are “gems among the junk” in DNA.¹⁴¹ Hence, a remaining question is whether use of junk DNA will continue to offer superficial identifying information or whether it will reveal more detailed medical or biological characteristics.

Conclusion

The nation, all 50 states, and many localities have adopted some type of DNA database program. Over time, Congress and state legislatures have expanded the types of crimes and the forms of police contact that result in DNA collection and databanking. Congress has demonstrated concern toward some aspects of DNA databanking by requiring expungement of a DNA profile in certain circumstances, prohibiting most non-forensic uses of DNA profiles and databases, and restricting familial searching. However, in general, Congress has taken a supportive attitude toward DNA databanking and incentivized the development, expansion, and integration of DNA databases.

As DNA database programs have widened in scope and grown in numbers, their consistency with the Fourth Amendment’s prohibition on unreasonable searches and seizures has increasingly been challenged. In the context of compulsory DNA collection, courts have widely upheld laws mandating the collection of DNA from persons who were convicted and are subject to the penal system’s custody or supervision. However, no judicial consensus has emerged regarding the constitutionality of mandating DNA collection from arrestees who have been criminally indicted. Instead, courts have split over the existence and scope of an arrestee’s reasonable expectation of privacy and the degree of privacy intrusion caused by DNA sampling. The limited number of court decisions in this area also suggests that there are conflicting opinions about the analogousness of DNA collection and fingerprinting.

Courts have generally upheld the indefinite use and storage of a lawfully databanked DNA profile after its source’s conviction. However, not all courts agree that *any* post-conviction use of those profiles is constitutionally acceptable. In particular, observers are now raising questions about the Fourth Amendment consistency of using databases for non-forensic purposes and for familial

¹³⁹ For example, in *Pool*, Judge Lucero wrote separately from the Ninth Circuit’s majority opinion to emphasize that, in the future, a litigant proved that a CODIS DNA profile yields information unavailable from a fingerprint or photograph, the “defendant’s interests could be vastly different” from Pool’s and the “totality-of-the-circumstances test” would need to be conducted anew. *Pool*, 621 F.3d at 1230-31 (Lucero, concurring). In *Kincade*, Judge Reinhardt wrote in his dissenting opinion that “The fact that scientists currently lack the capacity to comprehend the full significance of the data stored within junk DNA samples is irrelevant” to the Fourth Amendment analysis because the DNA profiles are retained forever and the advance of science will make them “only more revealing in time.” 345 F.3d at 850 (emphasis added).

¹⁴⁰ Lin L, Shen S, Tye A, Cai JJ, Jiang P, et al., *Diverse Splicing Patterns of Exonized Alu Elements in Human Tissues*, 4 PLoS GENETICS 1 (2008), <http://www.plosgenetics.org/article/info%3Adoi%2F10.1371%2Fjournal.pgen.1000225>.

¹⁴¹ W. Wayt Gibbs, *The Unseen Genome: Gems Among the Junk*, 29 SCI. AM. 49 (2003), <http://www.imb.uq.edu.au/download/large/TheUnseenGenome.pdf>.

searching. Currently, these concerns are largely confined to the scholarly literature—they have not come before a federal court—and are primarily centered on state database programs. Unlike some state DNA databases, the National DNA Index System (NDIS) and the Combined DNA Index System (CODIS) can not be used for either non-forensic research or intentional familial searching. However, the increase in states that authorize familial searching suggests that it may not be long before the constitutionality of familial searching comes before a federal court.

Much of the Fourth Amendment analysis of these issues depends on the current state of scientific knowledge on DNA and, more importantly, “junk” DNA—that is, the subset of DNA used to create databanked profiles. Decisions upholding DNA databanking programs have often described junk DNA as empty or meaningless genetic material because it is believed to reveal no sensitive information about its source. However, recent scientific research is challenging the accuracy of this description. While it may be too early for courts to treat this new research as fact, some have suggested that the constitutionality of DNA database programs should be reevaluated if “junk” DNA is ultimately found to reveal sensitive genetic information.

Author Contact Information

Emily C. Barbour
Legislative Attorney
ebarbour@crs.loc.gov, 7-5842

Acknowledgments

Portions of this report were originally authored by Anna C. Henning.