EMBRACING THE DNA FINGERPRINT ACT

PATRICK HAINES*

* Patrick Haines received his J.D. from the University of Colorado in 2007, and served as a Note and Comment Editor for the *Journal on Telecommunications & High Technology Law*. He thanks Judge Morris B. Hoffman, Judge Carlos A. Samour, Professor Philip J. Weiser, and Cynthia Sweet for their inspiration, support, and comments. Special thanks to Dr. Stefanie Krenz.

I. INTRODUCTION

The use of human deoxyribonucleic acid ("DNA") as evidence in criminal prosecutions is commonplace in this country and much of the world.[1] In addition to its use by police and prosecutors, DNA "fingerprinting" is an affordable and reliable tool of researchers in many sciences (medicine, biology, anthropology, etc.).[2] In this country, DNA evidence serves primarily to confirm the presence of identified suspects at crime scenes by matching their DNA to crime scene trace evidence.[3] In such "evidentiary use" scenarios, a suspect is compelled by warrant to provide a DNA sample after he has been identified through traditional police methods. If the suspect's DNA matches the crime scene biological evidence, the suspect's presence at the crime scene is confirmed.

The DNA fingerprints of convicted felons are currently saved in state and federal databases in accordance with state and federal law.[4] Using these databases, crime scene DNA evidence now serves a powerful "investigative use." When police find DNA evidence at a crime scene, potential suspects can be identified from the population of previously convicted felons by matching the crime scene DNA to databased DNA fingerprints. A suspect is identified when crime scene DNA matches either databased felon DNA or unknown DNA from another crime scene.[5] In this way, DNA evidence can generate suspects instead of merely confirming the presence of a known suspect at a crime scene. The match of crime scene DNA to an individual identified by his

1. *See* DNA RESOURCE, STATE DNA DATABASE LAWS: QUALIFYING OFFENSES (2003), *available at* http://www.dnaresource.info/documents/statequalifyingoffenses.pdf.

2. *See*, *e.g.*, Alan Cooper et al., *Ancient DNA: Would the Real Neandertal Please Stand Up*, 14 CURRENT BIOLOGY 431 (2004), *available at* http://download.current-biology.com/pdfs/0960-9822/PIIS0960982204003641.pdf; Yoshinori Kumazawa, *Mitochondrial DNA Sequences of Five Squamates: Phylogenetic Affiliation of Snakes*, 11 DNA RES. 137 (2004), *available at* http://dnaresearch.oxfordjournals.org/cgi/reprint/11/2/137.

3. Human Genome Project Information, DNA Forensics, http://www.ornl.gov/sci/techresources/Human_Genome/elsi/forensics.shtml (last visited Feb. 11, 2007) [hereinafter HGP].

4. *See, e.g.*, 42 U.S.C. § 14135 (2000); CAL. PENAL CODE § 296 (West 2006); LA. REV. STAT. ANN. § 15:609 (2006); NEB. REV. STAT. § 29-4103 (2006); N.J. STAT. ANN. § 53:1-20.20 (West 2007); TEX. GOV'T CODE ANN. § 411.1471 (Vernon 2006); VA. CODE ANN. § 19.2-310.2:1 (2006).

5. *See* Press Release, U.S. Dep't of Justice, Department of Justice Announces $98 Million in Grants for President Bush's DNA Initiative and Other Crime-Solving Forensic Services (September 19, 2005), http://www.ojp.usdoj.gov/pressreleases/NIJ05048.htm. Though matching DNA from one crime scene to another does not identify suspects directly, criminal investigators report that linking investigations through DNA expands opportunities for "case breaking" evidence to be identified.

databased DNA fingerprint is known as a "cold hit."[6] Predictably, the more DNA samples in the database, the better the statistical odds of obtaining a cold hit. Adoption of a federal "sample on arrest" policy for DNA fingerprinting will dramatically expand the number of potential cold hits. The benefits of a sample-on-arrest policy, including increased generation of suspect identities and increased case clearance rates, far outweigh the potential costs of such a policy to civil liberties and individual privacy.

The DNA Fingerprinting Act of 2005 ("Act"), passed as Title X of the Violence Against Women Act Reauthorization of 2005, requires anyone arrested for any federal crime to provide a DNA sample for analysis.[7] Other federal law requires DNA samples to be collected, analyzed, and databased from individuals convicted of certain crimes, mostly violent offenses.[8] The Act requires the government to collect, analyze, and store a DNA sample from anyone ***arrested*** for any federal crime.[9] Law enforcement will benefit from the increase in cold hits which should follow the resulting growth of the DNA fingerprint sample population. Persons arrested, however, are now compelled to provide a DNA fingerprint despite being presumed innocent; these individuals will bear the costs of potential Fourth Amendment infringements and potential threats to genetic privacy.

Passage of the Act signals that DNA is transcending its original evidentiary use, where it aided in the conviction of violent felons and exonerated the wrongly convicted, and is fast becoming primarily an investigative tool. Through the Act's federal "sample on arrest" policy, law enforcement will be poised to significantly increase the number of DNA fingerprints available for cold hit matching. The question remains whether such a policy is constitutional, and though no constitutional challenges to the Act have yet reached the federal Courts of Appeals, it is almost certainly only a matter of time before the question must be decided.

This note will first summarize the background of the DNA fingerprinting debate: the history of the use of DNA evidence, the

---

6. Mark A. Rothstein & Sandra Carnahan, *Legal and Policy Issues in Expanding the Scope of Law Enforcement DNA Data Banks*, 67 BROOK. L. REV. 127, 128 (2001).

7. Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, § 1004, 119 Stat. 2960, 3085 (codified as amended at 42 U.S.C. § 14135a).

8. *See* 42 U.S.C.A. § 14135 (2006). The current list of federal crimes that require offender submission of DNA samples may be found at 28 C.F.R. § 28.2 (2007).

9. 42 U.S.C.A. § 14135a (2006). The same section of the Act would also allow collection of DNA samples from "non-United States persons who are detained under the authority of the United States." *Id.* § 14135a(1)(A). This language is likely directed toward PATRIOT Act detainees and is outside the scope of this casenote, but such a provision certainly deserves further consideration and analysis.

corresponding federal legislation, and the adoption of DNA "John Doe" warrants. Next, the note will identify the DNA loci used for DNA fingerprinting, describe the process of DNA sample amplification and analysis, and summarize the statistics of sample matching. The note will also consider the debate over whether DNA fingerprints contain only "junk DNA," non-coding segments that reveal no sensitive information, or whether, as some argue, DNA fingerprints contain private information.

Following this background, the note will first rebut the criticism that the use of DNA fingerprinting in criminal trials is unfairly prejudicial and tends to sway juries that have become enamored with its reputation for accuracy and reliability. The note will then introduce the two major objections to a DNA sample-on-arrest policy: first, that the threat to the constitutionally-guaranteed personal privacy of individuals is too great; and, second, that the Fourth Amendment bar against unreasonable searches and seizures should preclude involuntary DNA sampling upon arrest.[10]

The note will discuss the text of the Act as signed into law on January 5, 2006. The note will argue that the Act withstands constitutional scrutiny under either a Fourth Amendment challenge or a "penumbra" privacy rights challenge. The note aims to show that these concerns are without merit, given the nature of the DNA samples taken, the existing procedural safeguards for both sampling and sample security, and the diminished privacy rights of arrestees. In conclusion, the note will address the major objections to the Act and reemphasize the benefits of a federal "sample on arrest" statute.

II. DNA EVIDENCE: LEGISLATION, APPLICATION, AND SCIENCE

A. A Brief History of DNA Evidence Legislation

The use of DNA evidence in criminal justice began in England in mid-1980s.[11] The first reported U.S. case to admit DNA evidence came in 1988.[12] Within a decade, virtually all state and federal jurisdictions in the U.S. were admitting DNA as evidence.[13] In 1994, the Violent Crime Control and Law Enforcement Act established a federal Combined DNA Index System ("CODIS") database, but did not authorize the collection

10. U.S. CONST. amend. IV ("The right of the people to be secure in their persons . . . against unreasonable searches and seizures, shall not be violated . . . .").

11. *See generally* Alec J. Jeffreys et al., *Individual-Specific '"Fingerprints'" of Human DNA*, 316 NATURE 76 (1985).

12. Andrews v. State, 533 So.2d 841 (Fla. Dist. Ct. App. 1988).

13. 2 PAUL C. GIANELLI & EDWARD J, IMWINKELRIED, SCIENTIFIC EVIDENCE § 18-5(A) (3d ed. 1999).

of DNA samples from anyone.[14] In 1996, proposed legislation intended to facilitate CODIS sample collection failed to pass through Congress, so CODIS remained idle.[15] Finally, in 2000, CODIS began to be systematically and reliably filled with DNA fingerprint data from qualifying convicts upon the enactment of the DNA Analysis Backlog Elimination Act ("Backlog Act").[16] The Backlog Act "authorize[d] a new program of Federal assistance to States to enable them to clear their backlogs of DNA samples . . . [and to] fill a gap in the system by authorizing collection, analysis, and indexing of DNA samples from persons convicted of Federal crimes."[17]

1. Current Federal and State DNA Collection Policies

Under the Backlog Act, individuals convicted for murder, manslaughter, sexual abuse, child abuse, kidnapping, robbery, burglary, or any attempt or conspiracy to commit such crimes, would be compelled to submit a DNA sample to CODIS.[18] All fifty states followed suit, enacting their own statutes requiring criminals to provide DNA to CODIS upon conviction of a qualifying crime.[19] Later, federal legislation added all violent crimes and terrorism to the qualifying list.[20] In practice, CODIS is maintained by the Federal Bureau of Investigation ("FBI"). Federal, state and local law enforcement can input qualifying DNA samples to CODIS, and can compare locally-collected crime scene DNA to the samples collected from known individuals and from other crime scenes that are retained in CODIS.[21]

14. Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, § 210304, 108 Stat. 1796, 2069 (codified as amended at 42 U.S.C. § 14132 (2000 & Supp. IV 2004)).

15. *See* Pub. L. No. 104-132, § 811(a)(2), 110 Stat. 1214, 1312 (1996); Pub. L. No. 105-251 (1996).

16. DNA Analysis Backlog Elimination Act of 2000, Pub. L. No. 106-546, § 3, 114 Stat. 2726, 2728 (codified as amended at 42 U.S.C. § 14135a).

17. H.R. REP. NO. 106-900, pt. 1, at 8 (2000).

18. § 14135a (d)(1).

19. *See, e.g.*, sources cited *supra* note 4. Note that state statutes often differ from federal statutes regarding qualifying crimes. While thirty-four states have an "all felonies" policy for DNA sampling of convicts, similar to the federal policy, thirty-eight states also allow some misdemeanors to qualify. At least four states (CA, LA, TX, VA) allow sample collection upon arrest for qualifying crimes. *See* SETH AXELRAD, AM. SOC'Y OF LAW, MED. & ETHICS, SURVEY OF STATE DNA DATABASE STATUTES (2004), http://www.aslme.org/dna_04/grid/guide.pdf (last visited April 12, 2007).

20. § 14135a (d)(2). The current list of qualifying federal crimes can be found at 28 C.F.R. § 28.2 (2007).

21. § 14132.

2. An Application of DNA to Criminal Justice: "John Doe" Warrants

DNA fingerprinting has gained sufficient acceptance within the mainstream to enable legislators to amend criminal statutes in favor of its use. For example, many states have passed statutes authorizing DNA "John Doe" warrants.[22] Such warrants toll statutes of limitation, for certain felonies, when a suspect is identified solely by the DNA fingerprint left at a crime scene.[23] The DNA fingerprint is used in lieu of name, alias, or physical description to identify the accused.[24] Once the warrant is issued, the case is considered "filed" and the statute of limitations tolls.[25] Such revisions to the statutes of many states result from widespread acceptance of DNA fingerprinting as proof of identity.[26]

"John Doe" is defined as a "fictitious name used in a legal proceeding to designate a person whose identity is unknown."[27] Courts have consistently upheld DNA John Doe warrants, finding that they do not violate due process and provide adequate notice to the suspect.[28] Some states have gone so far as to revise their statutes of limitation for violent felonies such that the statutes toll automatically upon identification of a suspect by his DNA.[29]

As statutes of limitation are revised such that they toll indefinitely upon DNA identification of a suspect,[30] one wonders if the original purposes behind statutes of limitation are being ignored altogether. The Model Penal Code describes statutes of limitation as necessary to protect civil rights by assuring that prosecutions will be based on "reasonably

---

22. *See* Meredith A. Bieber, Comment, *Meeting the Statute or Beating It: Using "John Doe" Indictments Based on DNA to Meet the Statute of Limitations*, 150 U. PA. L. REV. 1079, 1089 (2002).

23. State v. Dabney, 663 N.W.2d 366, 374–75 (Wis. Ct. App. 2003) (holding that an arrest warrant which identified defendant as "John Doe" with a specific DNA profile effectively tolled the six-year statute of limitations and satisfied requirements that an arrest warrant must, if the name of the person to be arrested is not known, designate that person by any description by which that person can be identified with reasonable certainty).

24. *Id.*

25. *Id.*

26. David Doege, *Novel Warrant IDs Suspect Only by DNA Databank Evidence Used to Charge "John Doe" in Rape*, MILWAUKEE J. SENTINEL, Sept. 2, 1999, at 1.

27. BLACK'S LAW DICTIONARY 853 (8th ed. 2004).

28. *See, e.g.*, *Dabney*, 663 N.W.2d at 375 (DNA John Doe warrant did not create any lack of notice issues such as would implicate due process considerations).

29. *See, e.g.*, COLO. REV. STAT. § 16-5-401 (8)(a.5) (2006) ("[I]n any case in which the identity of the defendant is determined, in whole or in part, by patterned chemical structure of genetic information, and in which the offense has been reported to a law enforcement agency, as defined in section 26-1-114(3)(a)(III)(B), C.R.S., within ten years after the commission of the offense, there shall be no limit on the period of time during which a person may be prosecuted after the commission of the offense . . . .").

30. *See, e.g.*, § 16-5-401 (8)(a.5).

fresh evidence."[31] Statutes of limitation "provide predictability by specifying a limit beyond which there is an irrebuttable presumption that a defendant's right to a fair trial would be prejudiced."[32] Proponents of DNA John Doe warrants rebut this challenge with the argument that, unlike eyewitness testimony, DNA evidence does not lose probative value over time.[33] Additionally, DNA evidence can be independently analyzed or a match disproved by the accused, even years or decades later.[34]

But such a policy allows the State's case to stay strong, based on crime scene DNA, while non-DNA evidence (e.g., witness recollection) that may exonerate the defendant is lost over time.[35] Consequently, defendants may be prejudiced by their inability to defend against a charge kept alive through an old, stale DNA John Doe warrant.[36] Additionally, no rational argument can be made that a DNA John Doe warrant puts a suspect on notice, except where the suspect actually committed the crime.[37] This pretext, of course, violates the most fundamental tenet of American jurisprudence: innocent until proven guilty.[38] Based on these arguments, the best control on the potential abuse of DNA John Doe warrants is to ensure that they are not issued unless the probability of conviction is sufficiently high in terms of all the non-DNA parts of the case (e.g., victim availability, police availability, other corroborating evidence) to support issuing such a warrant.[39]

Much has already been written arguing the benefits and detriments of DNA John Doe warrants.[40] The practice is considered within this note only to demonstrate that DNA fingerprinting has gained sufficient acceptance within the mainstream to enable legislators to amend statutes in favor of its use.

---

31. MODEL PENAL CODE § 1.06 cmt. 1 (1985).

32. Bieber, *supra* note 22, at 1089.

33. *Id.* at 1088.

34. DAVID H. KAYE & GEORGE F. SENSABAUGH, JR., REFERENCE GUIDE ON DNA EVIDENCE 506 (2001), *available at* http://www.fjc.gov/public/pdf.nsf/f385048e0431aa3c8525679e0055d35c/e527b2a2ac29ef1c85256a87004590b2/$FILE/sciman09.pdf.

35. *See* Tyler T. Ochoa & Andrew J. Wistrich, *The Puzzling Purposes of Statutes of Limitation*, 28 PAC. L.J. 453, 462 (1997).

36. *See, e.g.*, Veronica Valdivieso, Note, *DNA Warrants: A Panacea for Old, Cold Rape Cases?*, 90 GEO. L.J. 1009, 1042 (2002); Bieber, *supra* note 22, at 1079.

37. Bieber, *supra* note 22, at 1086.

38. *Id.*

39. Interview with Carlos Samour, Deputy Dist. Attorney, Colo. Second Judicial Dist., in Denver, Colo. (Sept. 19, 2005). I note with happiness that then-Deputy District Attorney Samour became Judge Samour, Colorado Eighteenth Judicial District, in December 2006.

40. *See, e.g.*, Corey E. Delaney, Note, *Seeking John Doe: The Provision and Propriety of DNA-Based Warrants in the Wake of Wisconsin v. Dabney*, 33 HOFSTRA L. REV. 1091 (2005); Lisa Schriner Lewis, Note, *The Role Genetic Information Plays in the Criminal Justice System*, 47 ARIZ. L. REV. 519 (2005); Bieber, *supra* note 22, at 1079.

B. The Science of Cold Hits and the "Junk DNA" Question

99.9% of human DNA is identical for all people, so DNA fingerprints must be selected from DNA sequences within the one tenth of one percent that differs between individuals.[41] Thirteen standard identifying loci are used for CODIS samples, representing about one one-millionth of the total human genome.[42] These thirteen loci contain repeated combinations of three to seven base pair units and are called short tandem repeats (STR).[43] Variation in the combinations of base pairs and number of repeats for each of the thirteen CODIS loci enables them to be individually identified.[44] The odds of any two people having identically matching STR at all thirteen CODIS loci approaches one in 575 trillion.[45]

Identification is rarely made on the basis of matching all thirteen loci.[46] Crime scene DNA is seldom that cooperative – DNA suffers degradation due to environmental conditions, contamination, etc. A satisfactory match of DNA fingerprints is declared when the maximum probability of a false match is less than the reciprocal of the U.S. population.[47] It can be stated with "reasonable scientific certainty" that a particular individual is the donor of a given DNA sample when this statistical test is satisfied.[48] Overall, based on the typical number of loci matched and the number of base pairs and repeats at each matched location, the odds of a false positive using the CODIS statistical method approach one in a billion.[49]

The fact that crime scene DNA may be degraded by any number of environmental factors makes it necessary to improve sample quality after collection.[50] The amplification of crime scene DNA samples is accomplished by polymerase chain reaction (PCR), which is described as:

> [a] molecular duplicating process that uses basic cellular chemistry

---

41. HGP, *supra* note 3.

42. David H. Kaye, Commentary, *Two Fallacies About DNA Data Banks For Law Enforcement*, 67 BROOK. L. REV. 179, 188 (2001).

43. HGP, *supra* note 3.

44. *Id.*

45. Sarah L. Bunce, Comment, *United States v. Kincade – Justifying the Seizure of One's Identity*, 6 MINN. J. L. SCI. & TECH. 747, 752 (2005). Note that the global human population is only about 6.5 billion. *See* U.S. Census Bureau, World POPClock Projection, http://www.census.gov/ipc/www/popclockworld.html (last visited Feb. 16, 2007).

46. HGP, *supra* note 3.

47. Bunce, *supra* note 45, at 752. The reciprocal of the U.S. population is approximately 1/301,000,000. *See* U.S. Census Bureau, *supra* note 45.

48. Bunce, *supra* note 45, at 752.

49. HGP, *supra* note 3.

50. *Id.*

> and enzymes to create millions of copies of a desired portion of DNA through repeated cycling of a reaction using heating/cooling. This process enables scientists to obtain DNA information from small or degraded specimens. In forensic science applications, specific sequences of DNA are targeted that are highly variable amongst different individuals [(i.e., the thirteen CODIS loci)].[51]

In other words, crime scene DNA samples that do not include a sufficient quantity of genetic material for accurate laboratory analysis can be duplicated over and over again until the sample size becomes sufficient for reliable analysis. The relatively short length of each STR segment makes it suitable for PCR.[52] After amplification with PCR, the DNA from a sample as small as a few skin cells can yield a reliable match.[53] Even highly degraded samples can often be analyzed – it only takes a few uncompromised cells to initiate successful sample amplification through PCR.[54]

1. "Junk DNA" Explained

Though the entire human genome has been mapped, only 1.4 percent of it is currently believed to contain functioning genes.[55] A gene is defined as a sequence of DNA base pairs that codes for a specific protein.[56] Some of the remaining 98.6% of human DNA may serve regulatory functions, and some non-coding DNA has been identified which indicates predisposition toward certain diseases.[57] However, scientists believe that a significant portion of this non-coding DNA may merely be parasitic DNA inserted by viruses or artifacts of genes made obsolete by human evolution.[58]

Because the thirteen loci used by CODIS do not code for any known protein or indicate any known disease predisposition, they have been described as "junk DNA."[59] This label is somewhat misleading. Some non-coding loci can indicate or predict disease states, and all loci (coding and non-coding alike) can be used for parentage testing.[60] Privacy

---

51. National DNA Databank Glossary, Polymerase Chain Reacton (PCR), http://www.nddb-bndg.org/glossaire_e.htm (last visited Feb. 16, 2007).

52. Bunce, *supra* note 45, at 751.

53. HGP, *supra* note 3.

54. *Id.*

55. Kaye, *supra* note 42, at 188.

56. HGP, *supra* note 3.

57. *See* Ann Gibbons, *Studying Humans – and Their Cousins and Parasites*, 292 SCI. 627, 628 (2001).

58. *Id.*

59. *See* United States v. Kincade, 379 F.3d 813, 837–38 (9th Cir. 2004); Kaye, *supra* note 42, at 188; HGP, *supra* note 3.

60. Kaye, *supra* note 42, at 187 (citing David H. Kaye, *Bioethics, Bench, and Bar: Selected Arguments in Landry v. Attorney General*, 40 JURIMETRICS J. 193 (2000), and R. L.

advocates argue that the STR sequences recorded in CODIS may someday yield information about an individual's medical predispositions, behavior, or heritage despite its non-coding nature, and should therefore be protected.[61] That is, some advocates argue that today's junk DNA may be tomorrow's "window on the soul."[62]

This claim is not yet supported by actual breakthroughs, though we know that non-coding loci can indicate parentage or predict disease states.[63] For example, the condition known as G6PD deficiency causes anemia in humans, and has two variants (of many) that are strongly associated with certain non-coding regions near the G6PD gene.[64] Though the non-coding region near the G6PD gene is not used for CODIS sampling, the fact that non-coding DNA has been shown to contain arguably private genetic information indicates how misleading the label "junk DNA" actually is. This fact suggests to many that the risks of widespread genetic profiling or indefinite retention of biological sample material may outweigh the benefits to the criminal justice system of DNA fingerprinting.[65]

Despite such concerns, there is currently no known potentially compromising genetic information contained among the thirteen CODIS locations other than the fact that they serve as a unique DNA fingerprint that can also confirm familial relationships.[66] The "parentage testing" aspect is sometimes raised by privacy advocates as a further argument against DNA fingerprinting – the fact that DNA can conclusively prove familial relation is held by some to be an intrusion into privacy.[67] However, no rational public policy argument can be offered against accuracy when it becomes the task of the judiciary to sort out parentage. The "window on the soul" argument tends to be the strongest criticism of DNA fingerprinting by privacy advocates, and will be discussed further below.

Alford et al., *Rapid and Efficient Resolution of Parentage by Amplification of Short Tandem Repeats*, 55 AM. J. HUM. GENETICS 190 (1994)).

61. *See* Mark A. Rothstein, *The Impact of Behavioral Genetics on the Law and the Courts*, 83 JUDICATURE 116, 117 (1999) (reporting that scientists are identifying genes that may indicate aggression, sexual orientation, and antisocial behavior).

62. *See id.*

63. *See* Gibbons, *supra* note 57, at 628.

64. *Id.*

65. *See, e.g.*, Press Release, ACLU, ACLU Alarmed At Justice Department Move to Collect DNA, Violates Privacy Rights and Causes Further Delays in Overwhelmed System (Feb. 5, 2007), http://www.aclu.org/privacy/gen/28251prs20070205.html.

66. *See generally* JOHN M. BUTLER, FORENSIC DNA TYPING: BIOLOGY AND TECHNOLOGY BEHIND STR MARKERS (2001); *see also* Kaye, *supra* note 42, at 188; HGP, *supra* note 3.

67. HGP, *supra* note 3.

2. The Possibility of Human Error in DNA Fingerprinting

The possibility of human error in human systems is inherent and should never be ignored. When weighing the value of forensic evidence, the role of human beings in the chain of custody must be considered.[68] As recently as May 2004, a high-profile error in fingerprint analysis by the FBI was acknowledged after an Oregon lawyer was wrongly identified as a participant in the Madrid, Spain train bombings.[69] The possibility of sample contamination at any step in the collection and analysis chain can never be forgotten. Likewise, samples may be mislabeled, mishandled, misplaced, misused or blatantly falsified, as with any crime scene evidence.

Beyond this possibility of human error in collecting, analyzing, and cataloging DNA samples, there remain legitimate questions about the infrastructure that supports DNA fingerprinting. There is well documented evidence of poor management, budget shortages, and corruption within crime labs.[70] In England in 1999, Raymond Easton, a formerly convicted burglar whose DNA fingerprint was on file was wrongly arrested on the strength of a four-loci DNA match between his DNA fingerprint and a sample collected from a crime scene.[71] Easton was charged with burglary based on the four-loci cold hit which, statistically, had only a one in thirty-seven million chance of being a false positive.[72] It was subsequently proven that Easton was two hundred miles away at the time of the crime; additionally, Easton suffered from advanced Parkinson's disease, making it medically impossible that he committed the burglary.[73] Further analysis revealed that two additional DNA loci did not match and Easton was exonerated.[74] Like traditional fingerprint evidence, DNA evidence is only as reliable as the people and processes by which it is collected and analyzed.

---

68. *See, e.g.*, Jennifer L. Mnookin, Op-Ed., *A Blow to the Credibility of Fingerprint Evidence*, BOSTON GLOBE, Feb. 2, 2004, at A14.

69. Susan Schmidt & Blaine Harden, *Lawyer is Cleared of Ties to Bombings: FBI Apologizes for Fingerprint Error*, WASH. POST, May 25, 2004, at A2.

70. *See, e.g.*, Adam Liptak, *The Nation; You Think DNA Evidence is Foolproof? Try Again*, N.Y. TIMES, Mar. 16, 2003, at D5.

71. Jennifer L. Mnookin, *Fingerprint Evidence in an Age of DNA Profiling*, 67 BROOK. L. REV. 13, 49–50 (2001).

72. *Id.*

73. *Id.*

74. *Id.*

III. CRITICISMS: JURY BIAS AND CONSTITUTIONAL PRIVACY

A. Raising and Rebutting the Jury Bias Argument

One criticism of DNA evidence echoes those heard following the introduction of fingerprint evidence at the beginning of the last century. When fingerprint evidence was first allowed by American courts, juries were often offered a "demonstration" of the art by the forensic expert, which often included the expert identifying the jurors themselves by their collected fingerprints.[75] Those demonstrations resembled sideshow mysticism more than *voir dire*, and juries could be blinded to the possibility of human error in this new forensic art by its dazzling power to accurately identify the jury's own members.[76]

DNA evidence is the target of similar criticism of disproportionate influence on juries. As it was with fingerprint evidence, forensic experts very often present DNA evidence in the language of fact, the patois of certainty, rather than in the language of scientific opinion.[77] The perception of DNA's infallibility is so pervasive in the popular culture,[78] it is argued, that the potential for human error during sample collection, preservation, and analysis is overlooked.[79]

While the possibility of human error should never be ignored by legal counsel, particularly in light of continuing fingerprint evidence errors, this possibility is adequately accounted for in our adversarial system. At least one high-profile case argued in recent memory resulted in a not guilty verdict despite "indisputable" DNA evidence.[80] Verdicts like that delivered in the O.J. Simpson murder trial provide at least anecdotal evidence that any prejudicial effect of DNA evidence is balanced by the inherent independence of the jury trial system.[81]

Furthermore, there is evidence that rather than being dazzled by

---

75. *See id.* at 24 (citing People v. Chimovitz, 211 N.W. 650 (Mich. 1927); Stacy v. State, 292 P. 885 (Okla. Crim. App. 1930); Hopkins v. State, 295 S.W. 361 (Ark. 1927)).

76. *Id.* at 26.

77. Mnookin, *supra* note 71, at 28–30.

78. *See* Dr. Kimberlianne Podlas, *"The CSI Effect": Exposing the Media Myth*, 16 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 429 (2006); *see also* Kit R. Roane, *The CSI Effect, How TV is Driving Jury Verdicts All Across America*, U.S. NEWS & WORLD REP., Apr. 25, 2005, at 48.

79. *See, e.g.*, Mnookin, *supra* note 68, at A14; Podlas, *supra* note 78, at 437.

80. *See, e.g.*, *CNN Presents: Simple as DNA* (CNN television broadcast Sept. 25, 1995), *available at* http://www.cnn.com/US/OJ/verdict/dna/ (last visited Feb. 16, 2007); *PBS Frontline: Interview with Gerald Uelmen* (PBS television broadcast Oct. 4, 2005) (interviewing former member of the O.J. Simpson defense team and former dean and current Professor of Law at Santa Clara University), *available at* http://www.pbs.org/wgbh/pages/frontline/oj/interviews/uelmen.html.

81. *News and Notes with Ed Gordon: 10 Years After the O.J. Verdict* (NPR Commentary by Clarence Page broadcast, Oct. 3, 2005)

DNA evidence, jury members are now probing sample chains of custody, challenging the credibility of laboratory analysts, and inquiring about the possibility of errors in DNA evidence where trials turn on such evidence.[82] Initially referred to by trial lawyers as the "CSI Effect,"[83] this alleged trend results from juries becoming more sophisticated and critical in their consideration of DNA evidence as forensic science becomes a staple of television news and entertainment.[84] At least one objective study in the legal literature suggests that the "CSI Effect" neither raises the bar for prosecutors attempting to use DNA evidence at trial, nor lowers it through DNA's reputation for infallibility, consistent with the anecdotal evidence discussed above.[85] It appears that the competing practical effects of DNA evidence use at trial cancel one another out. Disposing of the "jury bias" argument leaves us with two serious constitutional concerns.

B. Raising the Fourth Amendment Question

The Fourth Amendment right to be free from unreasonable government intrusion, as explained in *Katz v. United States*, requires a two-pronged analysis: first, a court must determine whether a person has exhibited a subjective expectation of privacy in the matter at issue; if so, the court then asks whether such expectation is ". . . one that society is prepared to recognize as 'reasonable.'"[86] The fact that DNA fingerprinting statutes now include far more felonies than originally contemplated by the Backlog Act,[87] as discussed in more detail below, suggests that our culture is becoming increasingly comfortable with the collection of DNA samples from an ever-widening segment of society.

The Fourth Amendment is implicated only if obtaining a DNA sample from an arrestee constitutes an unreasonable search.[88] DNA evidence found at a crime scene is not the fruit of a search, and is admissible as evidence pursuant to *Katz v. United States*.[89] In *Katz*, the Supreme Court held that what a person chooses to voluntarily expose to

---

82. Telephone Interview with Captain Julie Caruso, U.S. Army Judge Advocate Gen. Corps, in Wash. D.C. (Dec. 27, 2005); *see also* H. Patrick Furman, Clinical Professor of Law, Trial Advocacy Lecture at the University of Colorado Law School (Jan. 11, 2006).

83. H. Patrick Furman, *supra* note 82.

84. Podlas, *supra* note 78, at 461–65.

85. *Id.*

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

87. *Compare* source cited *supra* note 16, *with* sources cited *supra* note 20.

88. U.S. CONST. amend. IV ("The right of the people to be secure in their persons . . . against unreasonable searches and seizures, shall not be violated . . . .").

89. *Katz,* 389 U.S. at 347. Note also that biological samples and trace evidence are not testimonial, and therefore do not implicate the Fifth Amendment protection against self-incriminating testimony. *See* Schmerber v. California, 384 U.S. 757 (1966).

the public is not protected by the Fourth Amendment.[90] Biological evidence left by a perpetrator at a crime scene may be seized under the exigency exception to the Fourth Amendment,[91] may be determined to have been voluntarily exposed to the public in accordance with *Katz*, or may be lawfully searched and seized upon the consent of the crime scene property owner. Though rarely necessary under the exigence doctrine, a warrant can generally be obtained if needed to gain access to a crime scene. Regardless of the means by which law enforcement gains access to a crime scene, analysis of crime scene DNA does not implicate the Fourth Amendment with regard to the crime scene DNA donor. However, the involuntary collection of a DNA sample from a federal arrestee does raise the Fourth Amendment question of whether such a sample collection constitutes an unreasonable search of the person or seizure of the DNA.

The federal policy of collecting DNA samples from convicted felons has withstood constitutional challenge.[92] In *Landry v. Attorney General*, a constitutional challenge to the involuntary collection of DNA samples from convicted felons was defeated.[93] The Court held that collection of DNA samples in order to accurately establish the identity of criminals did not implicate the Fourth Amendment.[94] It is now also well settled that, on balance, the government's legitimate interest in an effective and accurate criminal justice system outweighs the diminished privacy rights of convicted felons, making collection of DNA samples from felons a minimal and constitutional intrusion.[95] However, no federal court has yet extended this balance to include arrestees.[96] Though four states have sample-on-arrest statutes, the Supreme Court has not yet considered the question of whether the "diminution of privacy rights" justification extends to arrestees. There is precedent, however, holding that arrestees already have a diminished expectation of privacy.[97] The question remains whether that diminished privacy expectation, when balanced against the government's legitimate interest

90. *Katz*, 389 U.S. at 351.

91. *See, e.g.*, *Schmerber*, 384 U.S. at 757.

92. Landry v. Attorney Gen., 709 N.E.2d 1085, 1092 (Mass. 1999).

93. *Id.*

94. *Id.*

95. *See, e.g.*, United States v. Kincade, 379 F.3d 813, 837–38 (9th Cir. 2004); Rise v. Oregon, 59 F.3d 1556, 1560 (9th Cir. 1995).

96. In *Kincade*, the court was careful to limit its holding to convicted felons, noting that "the DNA act implicates only the rights of convicted felons – not free persons or even mere arrestees." 379 F.3d at 836 n.31.

97. *See* Illinois v. Lafayette, 462 U.S. 640, 643 (1983) (holding that search incident to arrest constitutes a well-defined exception to the Fourth Amendment warrant requirement); United States v. Robinson, 414 U.S. 218 (1973); State v. White, 722 P.2d 118 (Wash Ct. App. 1986) (holding that once arrested, there is a diminished expectation of privacy in the person of the arrestee).

in solving crimes and apprehending criminals, is sufficiently low to allow an unwarranted search upon arrest.

C. Raising the Right to Personal Privacy Question

While the Fourth Amendment privacy question is clearly limited to the "search and seizure" elements of obtaining a DNA sample from a suspect, the personal privacy issue extends to the genetic information that remains unknown or unanalyzed in the biological sample itself. Though DNA fingerprint samples are analyzed for only the thirteen CODIS loci, the sample itself may still contain the entire balance of that individual's genetic code.[98] Because the Act (and its predecessors, such as the Backlog Act) allows the retention of biological samples following analysis, every sampled individual's genetic code potentially remains, unanalyzed, in the hands of the government.

There is a right to privacy that extends beyond the Fourth Amendment protections of privacy vested in persons and possessions. While the constitutional source of such right remains in debate, the Supreme Court has recognized for several years that a right of personal privacy does exist.[99] It is this right that protects individuals from governmental inquiry into matters in which government does not have a legitimate and proper interest.[100] However, the source and extent of this constitutional right to personal privacy remains hotly debated.[101]

The right to personal privacy is most often cited as the basis for the protection from government intrusion into marital intimacy,[102] sexual conduct among consenting adults,[103] the reading of "obscene" materials

98. HGP, *supra* note 3.

99. *See* Lawrence v. Texas, 539 U.S. 558, 595 (2003) (Scalia, J., dissenting) (explaining that the right to personal privacy is grounded in the penumbra of the Bill of Rights) (citing Eisenstadt v. Baird, 405 U.S. 438 (1972)); *see also* Roe v. Wade, 410 U.S. 113, 152 (1973) (holding that the right of privacy is founded in the Fourteenth Amendment's concept of personal liberty). Whether such a right to privacy derives from the Fourteenth Amendment or a constitutional penumbra has little bearing on the question as raised in this note. The personal privacy right protects "two kinds of privacy interests: the individual's interest in avoiding disclosure of personal matters and the interest in being independent when making certain kinds of personal decisions." Eastwood v. Dep't of Corr., 846 F.2d 627, 630–31 (10th Cir. 1988).

100. *See, e.g.*, *Eastwood*, 846 F.2d at 630–31; Whalen v. Roe, 429 U.S. 589, 599–600 (1977) ("The cases sometimes characterized as protecting 'privacy' have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions.").

101. *See, e.g.*, *Lawrence*, 539 U.S. at 595 (Scalia, J., dissenting); Griswold v. Connecticut, 381 U.S. 479, 508 (1965) (Black, J., dissenting) ("The Court talks about a constitutional 'right of privacy' as though there is some constitutional provision or provisions forbidding any law ever to be passed which might abridge the 'privacy' of individuals. But there is not.").

102. *See, e.g.*, *Eisenstadt*, 405 U.S. at 438; *Griswold*, 381 U.S. at 479.

103. *See, e.g.*, *Lawrence*, 539 U.S. at 558.

in the privacy of one's home,[104] and, of course, reproductive rights.[105] There is not yet any precedent holding that collection of a DNA sample for identification purposes implicates this limited right. While collection of a DNA sample is clearly a Fourth Amendment intrusion, it is not yet clear whether the analysis and storage of a DNA fingerprint from an arrestee will be held to implicate the limited constitutional right to personal privacy. If DNA fingerprints are proven to contain discernable personal information (i.e., if they open a "window on the soul") they would be more deserving of the protection of the limited constitutional right to personal privacy. Moreover, if the retained biological samples collected by law enforcement were to be further analyzed for anything other than CODIS loci, a significant personal privacy issue should be raised.

Privacy advocates argue that even the so-called junk DNA sequences recorded in CODIS may someday yield information about an individual's medical predispositions, behavior, or heritage that is private and should therefore be protected.[106] It is argued that such samples should be collected only from persons whose privacy rights have already been decreased by a criminal conviction, if they are to be collected at all.[107] Even with a "sample on conviction" policy, the argument continues, the biological samples themselves should be destroyed after analysis and codification of the DNA fingerprint. The biological samples, after all, likely contain all of the individual's DNA, not just the thirteen CODIS loci. Therefore, sensitive personal information compromising the individual's genetic privacy rights could be revealed by subsequent re-analysis, either by the FBI or by third parties who obtain the samples.[108]

Despite the above concerns, it appears neither DNA fingerprinting nor CODIS are likely to be abandoned anytime soon. Some objections to DNA evidence can be dismissed as either self-correcting or reflective of the inherent infirmities of human social systems (e.g., jury bias, human error). Current case law holds that the federal "sample on conviction" policy passes constitutional muster on the questions of privacy rights and Fourth Amendment protections. Therefore, two questions remain: (1) whether the "sample on arrest" policy is an unconstitutional intrusion into the genetic privacy of *arrestees* under the constitutional right to personal privacy; and (2) whether involuntary DNA sampling upon arrest

104. *See*, *e.g.*, Stanley v. Georgia, 394 U.S. 557 (1969).

105. *See, e.g.*, Carey v. Population Servs. Int'l, 431 U.S. 678 (1977); *Roe*, 410 U.S. at 113.

106. *See* Rothstein, *supra* note 61, at 117 (pointing out that scientists are identifying genes that may indicate aggression, sexual orientation, and antisocial behavior).

107. *Id.*

108. *See* Kaye, *supra* note 42, at 181 nn.9–11.

constitutes an unreasonable search and seizure under the Fourth Amendment.

IV. THE ARGUMENT IN FAVOR OF THE DNA FINGERPRINT ACT OF 2005

A. The DNA Fingerprint Act of 2005

The Act passed the House of Representatives as stand-alone legislation,[109] was incorporated into the Senate's reauthorization of the Violence Against Women Act,[110] and was signed into law by President Bush on January 5, 2006. The Act authorizes, *inter alia*, collection of DNA samples from persons arrested or detained under federal authority for inclusion in CODIS.[111] At least four states have already passed "sample on arrest" laws,[112] and it is likely that other states will adopt similar legislation now that the Act is federal law.[113] The pertinent parts of the Act appear as Title X of the Violence Against Women Act Reauthorization of 2005:[114]

> The Attorney General may collect DNA samples from individuals who are arrested under the authority of the United States. The Attorney General may collect DNA samples from non-United States persons who are detained under the authority of the United States.
> The Director of the FBI shall promptly expunge from CODIS the DNA analysis of a person against whom charges were dismissed upon receipt of a final court order.
>
> The Director of the FBI shall promptly expunge from CODIS the DNA analysis of a person against whom charges were dismissed, not filed within the applicable time period, or who was acquitted upon

109. DNA Fingerprint Act of 2005, Pub. L. No. 109-162, tit. X, 119 Stat. 2960, 3084; H.R. 2796, 109th Cong. (2005).

110. Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, § 1004, 119 Stat. 2960, 3085 (codified as amended at 42 U.S.C. § 14135a).

111. *Id.*

112. *See* CAL. PENAL CODE § 296 (West 2006); LA. REV. STAT. ANN. § 15:609 (2006); NEB. REV. STAT. § 29-4103 (2006); N.J. STAT. ANN. § 53:1-20.20 (West 2007); TEX. GOV'T CODE ANN. § 411.1471 (Vernon 2006); VA. CODE ANN. § 19.2-310.2:1 (2006). Virginia began taking DNA from arrestees in January 2003 and collects about 8,000 samples each year according to Richard Willing*, FBI May Collect Juveniles' DNA*, USA TODAY, Nov. 16, 2003.

113. *See, e.g.*, TIM SCHELLBERG & LISA HURST, APPLIED BIOSYSTEMS, DNA RESOURCE REPORT (2007), *available at* http://www.dnaresource.com/documents/2007_1.pdf. Prior reports posted at this website contain similar synopses of cases involving DNA evidence in the U.S. and abroad.

114. The Act is written as amendments to the DNA Identification Act of 1994 and is best understood within that context. *See* Pub. L. No. 103-322, 108 Stat. 2065 (codified as amended in 42 U.S.C.).

receipt of a final court order.

Simply stated, the Act empowers the Attorney General to collect samples from arrestees and detainees[115] and requires the Director of FBI, as manager of CODIS, to expunge the samples of arrestees that are not subsequently convicted. The statutory expunging requirement mitigates the privacy infringement that arguably results when DNA samples are collected from unconvicted persons, while still allowing ample time for arrestee DNA to be compared to crime scene DNA samples from other unsolved crimes.

B. Arguments in Favor of the Act

The criminal justice system derives many benefits from the use of DNA fingerprints. DNA fingerprinting provides a more positive form of identification than the collection of conventional fingerprints, mug shot photography, recording a physical description, or other conventional methods because there is no known method of altering or temporarily eradicating one's genetic code.[116] It has been argued that DNA data does, in fact, increase "the accuracy of the criminal justice system,"[117] and this is persuasive. If the accurate identification of persons in the custody of the federal government was the primary goal of CODIS, then taking DNA samples upon arrest for a federal offense would probably satisfy a "rational basis" test. But though it is unquestionably a valuable characteristic of CODIS, "accuracy" is only a secondary benefit of DNA fingerprinting.[118] The primary legislative intent behind CODIS is the generation of investigative leads.[119] Therefore, the Fourth Amendment question remains: does collection of a DNA sample upon arrest constitute an unreasonable search? If not, then the Act is likely constitutional.

1. Response to Fourth Amendment Challenges

Under a *Katz* analysis, collecting DNA fingerprints from federal arrestees violates the Fourth Amendment if it satisfies both prongs of a two-pronged test.[120] First, the arrestee must have a subjective

115. This language may be directed toward PATRIOT Act detainees and is outside the scope of this casenote, but it certainly deserves further consideration and analysis.

116. Of course, the fact that DNA cannot be altered or eradicated precludes a *Schmerber* justification for sampling upon arrest. Schmerber v. California, 384 U.S. 757 (1966). In *Schmerber*, the Court held that a search incident to a valid arrest can include blood testing (in this case, to determine blood alcohol content) where fruits or evidence might be destroyed or concealed if not recovered (in this case, by normal human metabolism). *Id.*

117. United States v. Reynard, 220 F. Supp. 2d 1142, 1167 (S.D. Cal. 2002).

118. Kaye, *supra* note 42, at 203.

119. *Id.*

120. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

expectation that his DNA fingerprint is private.[121] Assuming, *arguendo*, that the first federal arrestee subjected to the Act had such an expectation, the second prong of *Katz* asks whether such a privacy expectation is one that society is prepared to recognize as reasonable.[122] The Fourth Amendment analysis therefore turns on whether society recognizes as reasonable an arrestee's expectation of privacy for his DNA fingerprint. Given the current fascination with DNA use in criminal justice,[123] and the success of recent legislation which expanded the use of DNA to fight crime,[124] there is a legitimate argument to be made that society does not hold reasonable an arrestee's expectation that his DNA fingerprint is private. Particularly in light of other existing safeguards (e.g., probable cause still required), and the narrow tailoring of the statute (e.g., mandatory expunging of arrestee DNA fingerprints from CODIS upon acquittal), a sample on arrest policy may well satisfy the *Katz* test as a reasonable intrusion into Fourth Amendment privacy.

Both well-settled case law and recent precedents will limit the government intrusions into Fourth Amendment rights that may arise under the Act. In *Davis v. Mississippi*, the Supreme Court held in 1969 that fingerprints obtained during an illegal arrest and detention were inadmissible as evidence.[125] The Court reaffirmed this position in 1985 when it decided *Hayes v. Florida*.[126] Though fingerprinting was recognized as less intrusive into an individual's private life and thoughts than an interrogation, and likewise less harassing than repeated contacts by police, the Court still required probable cause under the Fourth Amendment before a suspect could be arrested in order to procure his fingerprints.[127] The Court recognized the probative value of fingerprinting, calling it "inherently more reliable and effective" than eyewitness identifications or confessions, but maintained that the relevance and trustworthiness of illegally obtained evidence could not outweigh the constitutional prohibitions against such use.[128] A suspect may not be "apprehended, detained, and forced to accompany police to another location to be fingerprinted without a warrant or probable

121. *Id.*
122. *Id.*
123. *See supra* note 78.
124. *See supra* notes 16–19.
125. 394 U.S. 721 (1969).
126. 470 U.S. 811, 813 (1985) (where there was no probable cause to arrest suspect, suspect did not consent to journey to police station, and there was no prior judicial authorization for detaining him, investigative detention at police station for fingerprinting purposes violated petitioner's rights under Fourth Amendment; hence, fingerprints taken were the "inadmissible fruits of an illegal detention").
127. *Davis*, 394 U.S. at 724.
128. *Id.*

cause."[129] These precedents should also apply to DNA fingerprinting, thereby preventing invalid arrest as a pretext for the collection of DNA samples.

The United States Court of Appeals for the Ninth Circuit recently reviewed a matter of first impression regarding warrantless searches in *United States v. Scott*.[130] The reasoning of that case further illustrates the commitment of the judiciary to Fourth Amendment protections that will still apply under the Act. The Ninth Circuit held that mandatory drug testing cannot be imposed as a condition of pretrial release because it would violate the Fourth Amendment requirement for probable cause.[131] While the government may detain an arrestee or require bond to ensure his presence at trial, the government may not extract waivers of constitutional rights in exchange for benefits such as pre-trial release, even when those benefits are fully discretionary.[132]

An individual's consent to a warrantless search is only valid if the search itself is reasonable, regardless of whether the individual consented to such a search as a condition of pretrial release.[133] Under this precedent, a person could not constitutionally consent to DNA fingerprinting as a condition of custodial release; the government would have to show probable cause for arrest prior to any DNA fingerprinting. Where *Davis* and *Hayes* should preclude wrongful arrest as a pretext to obtain DNA fingerprints, *Scott* should preclude coercive DNA fingerprinting as a condition of release from custody (though, if the custodial arrest was valid, the Act requires DNA fingerprinting without further consent).

These precedents suggest that Fourth Amendment protections remain adequate under the Act. The fact that an arrestee's DNA fingerprint may connect them to other crimes is of no consequence to the Fourth Amendment analysis; it is no different than an arrestee's traditional fingerprints connecting him to another crime. The clear legislative intent behind DNA fingerprinting is to generate investigative leads and improve the accuracy of the criminal justice system, which is analogous to traditional fingerprinting, and therefore, DNA fingerprinting should receive the same Fourth Amendment protections as traditional fingerprinting.[134] Though arrestees are presumed innocent, a

129. *Hayes*, 470 U.S. at 818–19 (Brennan, J., concurring).

130. 424 F.3d 888 (9th Cir. 2005), *amended by*, 450 F.3d 863 (9th Cir. 2005).

131. *Id.* at 893.

132. *Id.* at 890–91.

133. *Id.* at 893.

134. *See* Napolitano v. United States, 340 F.2d 313, 314 (1st Cir. 1965) ("Taking of fingerprints in such circumstances is universally standard procedure, and no violation of constitutional rights."); Smith v. United States, 324 F.2d 879, 882 (D.C. Cir. 1963) (holding that "a person in lawful custody may be required to submit to . . . fingerprinting . . . as part of

valid arrest necessarily satisfies the probable cause required to detain the arrestee to answer for a crime.[135] If an arrest is valid, the subsequent search of the individual incident to arrest is also valid.[136] A person validly arrested has diminished expectations of privacy as a result of his arrest and detention.[137] Under a *Katz* analysis, if society does not recognize an expectation of privacy in an arrestee's DNA, a "search" of an arrestee's DNA would not be unreasonable.

Even if society does recognize a reasonable expectation of privacy in an arrestee's DNA fingerprint under *Katz*, a Fourth Amendment balancing test that weighs the government's legitimate and narrowly tailored interest in obtaining DNA fingerprints against the arrestee's diminished privacy interest should favor the government. Unless, and until, DNA fingerprinting is proven to reveal more about an arrestee than a unique and unchanging identification code, the value of DNA fingerprinting far outweighs the privacy intrusion on the affected individuals.[138]

Some observers have compared DNA analysis by law enforcement, with its potential for revealing a vast quantity of personal genetic information, to the widespread abuses that followed the introduction of wiretapping as an investigatory tool.[139] In *Olmstead v. United States*, the Supreme Court held that wiretapping did not infringe on the Fourth Amendment unless a physical trespass was implicated.[140] Subsequent history is replete with abuses by law enforcement, arguably culminating with the current Administration's domestic spying scandal,[141] though

---

the routine identification process"). Interestingly, it may soon be possible to obtain DNA samples from the skin oils that form crime scene fingerprints. Like the saliva left on a cigarette butt found at a crime scene, DNA samples obtained from skin oils left on surfaces would not implicate the Fourth Amendment under *Katz* because such oils would arguably have been exposed to public view, just like the other crime scene evidence. If no bodily intrusion was necessary to collect a DNA sample (i.e., if a suspect's skin oils were deposited on a paper coffee cup which the suspect then discarded), would its analysis and inclusion in CODIS as a DNA fingerprint be treated under Katz as if it were exposed to the public? *See* Rothstein & Carnahan, *supra* note 6, at 144–45.

135. Cupp v. Murphy, 412 U.S. 291, 301 (1973) (Douglas, J., dissenting in part) (defining arrest as "the taking of a person into custody so that he may be held to answer for a crime.") (citing OR. REV. STAT. § 133.210 (1972)).

136. Illinois v. Lafayette, 462 U.S. 640, 643 (1983) (affirming that a search incident to arrest constitutes a well-defined exception to the Fourth Amendment warrant requirement).

137. State v. White, 722 P.2d 118 (Wash. Ct. App. 1986).

138. Judge Morris B. Hoffman of the Colorado Second Judicial District raises the interesting question of whether the Fifth Amendment might one day be implicated by DNA. If DNA fingerprints are found one day to reveal evidence of a genetic propensity toward violence or sexual deviancy, or any "antisocial" trait, would that information become "testimonial" and therefore subject to Fifth Amendment analysis? This question is not ripe at present, given our limited understanding of the human genome, but is certainly worthy of further consideration.

139. *See generally* Kaye, *supra* note 42, at 193.

140. 277 U.S. 438, 466 (1928).

141. *See, e.g.*, Eric Lichtblau & James Risen, *Domestic Surveillance: The Program; Spy*

Olmstead has since been overruled and wiretapping is now much more tightly regulated.[142]

But DNA databases do not interfere with personal communication or track a person's movements like intercepted communications. Justice Brandeis' later-validated concerns with widespread wiretapping, expressed in his *Olmstead* dissent,[143] are not implicated by the Act because, unlike *Olmstead*-era wiretapping, there are now sufficient Fourth Amendment protections recognized by the judiciary to prevent the abuses that followed *Olmstead*.[144] Fourth Amendment fears must be balanced against the potential benefit of identifying offenders more quickly, potentially before their criminal conduct recurs or escalates, based on trace evidence that matches a CODIS sample.

2. Response to "Penumbra" Personal Privacy Challenges

As already discussed, the legislative intent behind the creation of CODIS was primarily to generate leads in criminal investigations. The expanding use of DNA evidence to generate suspects, rather than solely to support the prosecution of individuals already charged with crimes, fuels fears of diminished personal privacy resulting from DNA sample collection and storage.[145] The Act proposes to greatly expand the number of persons affected by DNA fingerprinting, whose entire genetic code would remain potentially intact, though unanalyzed, in the stored biological sample. The potential for abuse of such information cannot be ignored. Accordingly, this analysis must consider and resolve these personal privacy issues.

There is evidence that privacy concerns are overstated. Biological samples have long been used by forensic scientists to identify individuals.[146] For example, blood proteins and serum groups have long been accepted as forensic evidence even though such samples can contain the entire genetic code and other potentially sensitive biological

---

Agency Mined Vast Data Trove, Officials Report, N.Y. TIMES, Dec. 24, 2005, at A1; *see generally* BOB WOODWARD & CARL BERNSTEIN, ALL THE PRESIDENT'S MEN (1974) (describing illegal wiretapping by Presidential order at the Watergate Hotel).

142. *See Katz*, 389 U.S. at 347; Berger v. New York, 388 U.S. 41 (1967).

143. *Olmstead*, 277 U.S. at 474–75 ("[I]n the application of a Constitution, our contemplation cannot be only of what has been, but of what may be . . . [i]t is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty and private property . . . .").

144. *See* Kaye, *supra* note 42, at 193.

145. *See* Richard Willing, *Bill Would Expand U.S. DNA Database*, USA TODAY, Oct. 2, 2005, *available at* http://www.usatoday.com/news/washington/2005-10-02-dna-database-bill_x.htm.

146. Kaye, *supra* note 42, at 187.

information.[147] In the words of Professor David H. Kaye, a frequent and respected contributor to this debate, "[i]t serves no clear purpose to bar access to [DNA] loci that are not indicative of features of some social concern."[148]

Likewise, there are no known instances of CODIS data disclosure to any inappropriate third party.[149] Though no electronic database, federal or otherwise, can ever be completely secure in the Internet Age, it is unreasonable to declare CODIS data to be a significant risk to individual liberty and privacy in the absence of a documented wrongful disclosure or even a credible threat. Consider also that the U.S. Department of Defense has maintained a database of DNA fingerprints for all service members, for the purpose of identifying remains, since the late 1980's[150] with no known instances of inappropriate disclosure. In short, there is not yet compelling evidence that individual privacy will be compromised by DNA fingerprinting of arrestees. Note that when forensic fingerprinting first gained popularity, it was proposed that the secrets of an individual's heritage and personality could be deciphered from his fingerprints.[151] These claims were proven unfounded, and fingerprinting was ultimately accepted as the benign identification tool that we recognize today.[152] Additionally, the fact that DNA is color-blind should weigh in favor of the Act.[153]

The other source of concern is the biological samples themselves. These have the potential to reveal far more information than the CODIS fingerprint because the entire genome may exist within the sample.[154] The FBI opposes the destruction of stored biological samples, though these are arguably the most potentially sensitive element of the DNA

147. *Id.*

148. *Id.*

149. Searches of Westlaw, Lexis-Nexis and other resources revealed no reports of CODIS data compromise as of February 2007. As author M. Dawn Herkenham explains, "[t]he unauthorized disclosure of DNA information is subject to a criminal fine not to exceed $250,000, or imprisonment for a period not to exceed one year. Obtaining DNA samples or DNA information, without authorization, is punishable by a maximum fine of $250,000 or imprisonment for not more than one year or both fine and imprisonment." M. Dawn Herkenham, *Retention of Offender DNA Samples Necessary to Ensure and Monitor Quality of Forensic DNA Efforts*, 34 J.L. MED. & ETHICS 380, 382 (2006) (citing 42 U.S.C. §§ 14133(c), 14135e(c) (2004)).

150. U.S. Dep't of Def. Instruction No. 5154.30, Armed Forces Institute of Pathology Operations (Mar. 18, 2003), *available at* http://www.dtic.mil/whs/directives/corres/pdf/515430p.pdf.

151. *See* Mnookin, *supra* note 71, at 33–34.

152. *Id.*

153. Kaye, *supra* note 42, at 196. For example, a New Orleans murder suspect was believed to be African American, based on witness statements, until crime scene DNA showed he was Asian.

154. HGP, *supra* note 3.

fingerprinting process.[155] Reasons for the FBI's opposition include:

(1) to maintain uniformity among the states, because virtually all states require sample retention; (2) to avoid the prohibitive cost of re-typing convicted offenders once they have been released from prison, should it be necessary; (3) to assure data base consistency among the states in light of technological advances; (4) to allow re-checking a hit against the sample to assure a sample has not been mistyped, thus avoiding the release of a person's name to law enforcement personnel by mistake; and (5) that it is safe to retain samples because no abuse of stored samples has been reported in over ten years of databasing.[156]

Ironically, the assertion that CODIS, like any electronic database, should not be considered completely secure against electronic penetration may be the strongest argument in favor of biological sample retention. In the event that CODIS were compromised, the biological samples would remain as low-tech backups. If retained DNA samples are abused, through government analysis beyond the thirteen CODIS loci or release to third parties, the simplest and most expedient solution is to destroy the biological samples once the CODIS fingerprint is determined.

Privacy advocates often cite the increasing body of knowledge regarding genetic predispositions, such as an alcohol addiction predisposition, as a basis for genetic privacy fears.[157] To suggest that such genetic predispositions would prejudicially affect an individual's treatment by the criminal justice system ignores our system of law. Our legal system judges people on the basis of their conduct, not their genes.[158] Our criminal justice system is predicated on a belief in free will, not genetic predisposition.[159] The Federal Rules of Evidence already bar the use of "conformity" evidence with regard to character[160]; evidence of "genetic conformity" should similarly be barred. Additionally, many states already have "genetic property rights" statutes,[161] and equivalent federal law is being considered to prevent against wrongful possession or use of genetic information.[162]

---

155. Dr. Tom Callaghan, Program Manager, FBI, Remarks to the National Commission on the Future of DNA Evidence (Sept. 26, 1999), *available at* http://www.ojp.usdoj.gov/nij/topics/forensics/events/dnamtgtrans7/trans-c.html.

156. *Id.*

157. *See, e.g.*, Lee M. Silver, *The Meaning of Genes and "Genetic Rights"*, 40 JURIMETRICS J. 9, 17–18 (1999).

158. *See, e.g.*, Lewis, *supra* note 40, at 544.

159. *Id.*

160. FED. R. EVID. 404 (a)-(b) (prohibiting admission of character evidence to show conduct in conformity therewith).

161. *See, e.g.*, COLO. REV. STAT. § 10-3-1104.7 (2006) ("Genetic information is the unique property of the individual to whom the information pertains."); S.C. CODE ANN. § 38-93-30 (1998); Kaye, *supra* note 42, at 181 n.5.

162. *See, e.g.*, H.R. 1227, 109th Cong. (2005); S. 306, 109th Cong. (as passed by Senate, Feb. 17, 2005).

Currently, there is no compelling evidence that DNA fingerprinting will compromise personal privacy if its collection were to include arrestees; however, evidence that adding arrestees to CODIS will generate increased cold hits is undeniable. The FBI claims a cold-hit rate of only twenty-two percent using CODIS.[163] United Kingdom law enforcement officials, who follow a "sample on arrest" policy, claim a cold-hit rate of almost forty percent.[164] Most cold matches in England and New Zealand, where "sample on arrest" policies have been in place for years, come between crime scene DNA and the DNA fingerprints of burglary suspects and convicts.[165] Recidivism rates for felons are high and repeat offenders are common; more importantly, many persons ultimately convicted of violent felonies were previously arrested for lesser crimes, but released.[166] By expanding the CODIS population to include arrestees, the chances of a cold hit will increase based on the established patterns of repeat criminal conduct.

Finally, and perhaps most importantly, the Act requires the expunging of DNA fingerprints from CODIS for those persons who are exonerated, against whom charges are dropped, or against whom charges are not filed within the required time period.[167] In this way, the impact of the Act on the legitimate privacy concerns of innocent parties is mitigated.[168]

On balance, the benefits of the DNA Fingerprinting Act of 2005

---

163. *See* Federal Bureau of Investigation – Combined DNA Index System (CODIS) Home Page, http://www.fbi.gov/hq/lab/codis/index1.htm (last visited Apr. 2006) (noting that 27,700 cold hits had been generated from 124,285 crime scene DNA samples as of Nov. 2005).

164. Press Release, Forensic Sci. Serv., Crime Reduction Model (July 14, 1999) (on file with author).

165. *See*, *e.g.*, S.A. Harbison et al., *The New Zealand DNA Databank: Its Development and Significance as a Crime Solving Tool*, 41 SCI. & JUST. 33, 36 (2001) (reporting that 77% of reported database matches in New Zealand originated from burglaries); David Werrett, The Strategic Use of DNA Profiling, Address to the 18th International Congress of Forensic Haemogenetics (Aug. 19, 1999).

166. *See* LAWRENCE A. GREENFELD, U.S. DEP'T OF JUST., SEX OFFENSES AND OFFENDERS: AN ANALYSIS OF DATA ON RAPE AND SEXUAL ASSAULT 26–27 (1997) (rates of re-arrest and re-conviction for rapists were 52% and 36%, respectively; for all violent offenders, rates were 60% and 42%, respectively).

167. Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, § 1002, 119 Stat. 2960, 3084-85 (codified at 42 U.S.C. § 14132).

168. *See also UK Police Chief Calls for a National DNA Database*, 393 NATURE 106 (1998); *but see* David H. Kaye & Michael E. Smith, *DNA Identification Databases: Legality, Legitimacy, and the Case for Population-Wide Coverage*, 2003 WIS. L. REV. 413 (2003); Akhil Reed Amar, *A Safe Intrusion*, AM. LAW., June 2001, at 69 (advocating establishment of DNA data bank for all citizens, but requiring some of the precautions considered in this note, such as destruction of samples after analysis and analyzing only non-coding regions of the genome). The "expunging" provision of the Act is a significant factor in the balance favoring adoption of the Act; the absence of such a provision tilts the balance away from universal DNA sampling.

outweigh the risks. The balance between the competing interests of solving crimes and assuring genetic privacy must tilt toward optimizing the identification of criminal suspects, unless the privacy intrusions predicted by some to arise from DNA collection become manifest. Furthermore, Fourth Amendment concerns prove groundless once it is shown that DNA sample collection and analysis does not violate a detainee's diminished expectation of privacy. If privacy concerns are satisfied, then DNA fingerprinting can reasonably be treated as a "high-tech" alternative to traditional fingerprinting and employed in a constitutionally similar manner. Absent legitimate privacy concerns predicated on the compromise of CODIS data or the wrongful release of biological samples (which could be destroyed if necessary to prevent such a potential release), the constitutional protections against obtaining traditional fingerprints as the fruit of an unreasonable search should be adequate to protect against the abuse of DNA fingerprinting.

V. CONCLUSION

The DNA Fingerprint Act of 2005 adds the DNA fingerprints of persons arrested for federal offenses to CODIS, greatly expanding the CODIS sample population and thereby increasing the probability of obtaining cold hits. This approach is practiced in the United Kingdom and other western nations, which report cold-hit rates between crime scene DNA and individual DNA of almost double the rate such matches are generated in the United States. There is no reason not to expect similar success in suspect generation through crime scene DNA matching in this country. The one practical objection to the increased use of DNA in criminal justice that is not true of all forensic evidence is the claim that the persuasive power of DNA evidence outweighs its probative value. However, there is sufficient anecdotal evidence to illustrate that juries treat DNA evidence as skeptically as any other forensic evidence. In fact, emerging trends may indicate that the popular culture's fascination with DNA evidence may actually have raised the bar on its acceptance by juries.

The two principled objections to adopting a "sample on arrest" policy turn on privacy. Though a Fourth Amendment argument is often raised when the issue is debated, DNA fingerprinting is not fundamentally different from traditional fingerprinting once the privacy questions are resolved. The Fourth Amendment protections against illegal search and seizure that prohibit taking an individual's fingerprints without probable cause should extend to that individual's DNA fingerprint. Therefore, the Fourth Amendment issue should be well settled under existing case law by analogizing DNA fingerprinting to traditional fingerprinting.

The real issue is whether collection and retention of a biological sample, and the codification of a DNA fingerprint from that sample, creates an unbearable risk to individual liberty and personal privacy for persons presumed innocent. Persons convicted of felonies have diminished privacy and liberty rights, so the minimally-intrusive collection of their DNA fingerprints does not raise a constitutional question. But arrestees remain innocent until proven guilty, so the collection and analysis of DNA from arrestees raises privacy questions if their DNA fingerprints contain information worthy of constitutional protection.

Our society does not consider information that describes height, eye color, hair color, etc., to be worthy of privacy protection. Likewise, identification by fingerprints has long been accepted as minimally intrusive and unworthy of privacy protection (though, of course, protected by the Fourth Amendment). If we are to treat DNA fingerprints differently, that treatment must be based on a reasonable belief founded on actual events that the information contained in our DNA fingerprints is worthy of privacy protection. Though new discoveries about the content of our genetic code are frequently announced, science has not yet shown that the thirteen CODIS loci contain any information worthy of constitutional protection. Additionally, the CODIS database itself (and private genetic databases, for that matter) have, thus far, not been the target of significant acts of fraud or data compromise.

Likewise, the biological samples themselves, which the FBI retains after analysis, create no more risk to individual liberty and privacy than a blood sample provided to a physician – while both likely contain the entire genetic code of the donor, both are safeguarded against compromise. In fact, blood protein matching and serum typing has played a role in both civil and criminal jurisprudence for generations, so the use of biological sampling is hardly unprecedented. Add in the fact that DNA fingerprinting is "color-blind," has exonerated a significant number of wrongly-convicted individuals, does not degrade over time like most evidence, supports the issuance of "John Doe" warrants to ensure that justice can be done, and provides a unique and precise means of accurate identification when correctly interpreted, and the balance clearly favors the constitutionality of the Act.