"BANKING" ON LAW ENFORCEMENT: ADVOCATING A NEW BALANCING TEST FOR DNA STORAGE AFTER *UNITED STATES v. KINCADE*

INTRODUCTION

In a final effort to uncover the three-year mystery of a Cape Cod woman's murder, Truro, Massachusetts police investigators turned to the science of DNA analysis.[1] In January 2005, local police attempted to obtain so-called voluntary DNA samples from every man in the seaside town, totaling around 790 individuals.[2] The strategy was to match a sample of voluntarily extracted DNA with its perfect replica deposited on the body three years prior.[3] While the police assured local volunteers of their intentions to discard any DNA not matching the crime-scene sample, several Truro residents were skeptical of the promise that their genetic material would not become an entry in a state-wide or national database.[4] This DNA "dragnet" tactic is not commonly used in the United States, but has yielded results in England and Germany.[5] The use of individual DNA

---

1. Pam Belluck, *To Try to Net a Killer, Police Ask a Small Town's Men for DNA*, N.Y. TIMES, Jan. 10, 2005, at A1. *See also* Kathleen Burge & John Ellement, *Police Seek DNA Samples in 2002 Truro Slaying*, BOSTON GLOBE, Jan. 8, 2005, at B1; Eileen McNamara, *Flunking the Swab Test*, BOSTON GLOBE, Jan. 9, 2005, at B1.

Deoxyribonucleic acid ("DNA") is genetic information contained in all of an organism's cells, other than mature red blood cells. ELECTRONIC PRIVACY INFORMATION CENTER, GENETIC PRIVACY, http://www.epic.org/privacy/genetic (last visited Oct. 19, 2005) [hereinafter GENETIC PRIVACY]. "DNA provides exact instructions for the creation and functioning of the organism. DNA molecules of all organisms contain the same basic physical and chemical components, arranged in different sequences. The genome is an organism's complete set of DNA." *Id.*

2. Belluck, *supra* note 1.

3. *Id.*

4. *Id.* "'I really think they're usurping my civil rights,' said [Dick Seed, 44, a Truro sign painter who contacted the American Civil Liberties Union with concerns] . . . 'Are they going to chase down everyone who didn't give a sample? It kind of sounds like Stalin's secret police. If there's a murder committed in a restroom, are they going to be asking for a urine sample?'" *Id.* Incidentally, Truro law enforcement did have a sample from the suspect for over a year, but had prioritized processing samples from the dragnet over the backlog. Letter from Sujatha Byrayan, Ph.D., President, Council for Responsible Genetics, to Senate Judiciary Committee on the DNA Fingerprint Act of 2005 (Nov. 5, 2005), *available at* http://www.gene-watch.org/press/DNADatabase11-7-05.html.

5. *See* Belluck, *supra* note 1; Christine Rosen, *Liberty, Privacy, and DNA Databases*, THE NEW ATLANTIS, A JOURNAL OF TECHNOLOGY & SOCIETY, 37 (2003), *available at* http://www.thenewatlantis.com/archive/1/rosen.htm.

The first "dragnet" in history occurred in the wake of a "brutal rape and murder of two young women in the small English village of Narborough in 1986." *Id.* at 39. The process of solving the crime had the effect of revolutionizing criminal justice: the police caught the killer through analysis of

in this manner, while an undeniable boon for solving "cold" (inactive) cases with scientific accuracy, had local residents and the American Civil Liberties Union of Massachusetts perturbed at the potential ramifications of this privacy invasion.[6]

DNA databases have taken root in the United States both federally and across all fifty states.[7] Law enforcement agencies across the globe continue to reap benefits of a computerized system that can match genetic material lifted from a crime scene and produce a "cold hit," identifying a perpetrator whose profile exists in the database, as well as store unidentified samples for future use.[8]

A confluence of factors is currently setting the stage for vast expansion of DNA profiling in criminal justice. The mapping of the human genome

---

DNA. *Id*. During their investigation, the police used a DNA fingerprinting method developed by British scientist Alec Jeffreys to track down the perpetrator. *Id.* In so doing, they initiated the world's first genetic "dragnet," blood-testing more than 4,000 men in Narborough and the surrounding area until they located the genetic match: the killer. *Id.*

In the wake of the new technique's rousing success, the United Kingdom created a national criminal database in 1995. *Id.* As of May 2004, it houses approximately 2.58 million DNA profiles of convicted felons. POLICE REFORM UNIT, POLICE BRIEFING (Sept. 2004), http://www.police reform.gov.uk/docs/pbsep046.html (last visited Nov. 14, 2004); *see also* THE POLICE SCIENCE & TECHNOLOGY STRATEGY: 2004–2009, Aug. 24, 2005, at 15, http://www.policereform.gov.uk (follow "Publications" hyperlink under "News & Publications"; then follow "Operational Policy" hyperlink; then search list); *id.* at 14 (international comparison of percentage of total population profiled depicts the UK well in the lead at around 3.7%, followed by Austria, Switzerland and the U.S.).

The British database includes samples from crime scenes, from anyone convicted of a crime, and suspects in unsolved cases. Rosen, *supra*. British officials estimate that it will eventually include one-third of all English men between the age of sixteen and thirty. *Id.* Originally focused on sex offenders, the database eventually spread rapidly to include burglaries and car thefts. *Id.* The nation subscribed to the theory that catching petty criminals before their crimes escalate in violence might prevent more serious crimes down the road. Specifically,

> DNA databanks are premised on statistics indicating that individuals convicted of a serious violent offense often commit other violent offenses that leave behind incriminating DNA . . . In effect, databanks provide a means of genetically frisking anyone who has ever committed a covered offense for any crime in which DNA has been recovered.

Jonathan Kimmelman, *Just a Needle-Stick Away: DNA Testing Can Convict the Guilty; It Can Also Destroy the Privacy of Millions*, THE NATION, Nov. 27, 2000, at 17.

The United Kingdom police have recently proposed a universal DNA database that would include all residents. *See* GENETIC PRIVACY, *supra* note 1.

6. Belluck, *supra* note 1. Barry Steinhardt, director of the technology and liberty project at the American Civil Liberties Union, was also concerned: "They're not very effective and they're certainly not voluntarily [sic] . . . It's either give a sample or you're a suspect. It turns the classic American concept of innocent until proven guilty on its head." *Id.*

7. *See, e.g.*, Virna M. Manuel, Note, *State DNA Data Base and Data Bank Expansion Laws: Is it Time for California to Expand its DNA Data Base Law to Include All Convicted Felons?*, 31 W. ST. U. L. REV. 339, 346–49 (2004) (providing an overview of database statutes and states with expanded DNA databases).

8. *See generally* NATIONAL INSTITUTE OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, U.S. DEP'T OF JUSTICE, NIJ SPECIAL REPORT: USING DNA TO SOLVE COLD CASES (July 2002) [hereinafter NIJ SPECIAL REPORT].

offers numerous possibilities to discover genetic predispositions to disease, behavior, and even crime.[9] The United States' current involvement with the "war on terror" may serve to relax constitutional strictures barring invasions of privacy.[10] Moreover, the global community has entered a new age of technological advances that could not have been contemplated a few decades ago, making the repercussions of large-scale computerized storage of genetic material more pressing in the wake of court cases that have approved forced DNA extraction for various groups of criminals.[11]

The 2004 Ninth Circuit en banc decision of *United States v. Kincade* upheld the federal law requiring criminals on parole, probation, or supervised release to be forced to give DNA samples to the national DNA database regardless of any individualized suspicion.[12] The *Kincade* court grappled with Supreme Court opinions evaluating the reasonableness of searches under the Fourth Amendment.[13] However, none of the cases discussed in *Kincade* relating to "searches" involved the unique facet of DNA databanking: permanent computerized storage of private information.[14]

---

9. COUNCIL ON RESPONSIBLE GENETICS, GENETIC DISCRIMINATION: POSITION PAPER (2001), http://www.gene-watch.org/educational/genetic_discrimination.pdf [hereinafter CRG POSITION PAPER]. The goal of the multi-billion dollar Human Genome Project has been "to identify and sequence all of the genes that make up the human genome. *Id.* Much of this research focuses on genetic diagnostics: tests designed to identify genes thought to be associated with various medical conditions." *Id.* "The discoveries of the Human Genome Project are already shaking the foundations of our legal system, particularly in the area of criminal law." Lindsy A. Elkins, Note, *Five Foot Two With Eyes of Blue: Physical Profiling and the Prospect of a Genetics-Based Criminal Justice System*, 17 NOTRE DAME J.L. ETHICS & PUB. POL'Y 269, 296 (2003).

10. *See generally* NANCY CHANG, SILENCING POLITICAL DISSENT: HOW POST-SEPTEMBER 11 ANTITERRORISM MEASURES THREATEN OUR CIVIL LIBERTIES (Seven Stories Press) (2001); Nancy Chang, *The USA PATRIOT Act: What's so Patriotic About Trampling on the Bill of Rights?*, 58 GUILD PRAC. 142 (2001) [hereinafter Chang, *Trampling on the Bill of* Rights] (arguing that the USA Patriot Act "portents a wholesale suspension of civil liberties that will reach far beyond those who are involved in terrorist activities"). Chang argues that the Act launches a three-pronged assault on privacy, by 1) augmenting the surveillance powers of the executive branch; 2) permitting law enforcement agencies to gain warrants for searches and seizures based on a "significant purpose," rather than "probable cause as required under the Fourth Amendment; and 3) sharing information between criminal and intelligence operations. *Id.* The relaxation of standards with which law enforcement is required to comply may serve to launch a holding like the *Kincade* decision, discussed *infra*, into a rationale for significant DNA database expansion.

11. *See infra* note 119 and accompanying text. *See also* Jeffrey Rosen, *Roberts v. The Future*, N.Y. TIMES, Aug. 28, 2005, § 6 (Magazine), at 24 (discussing technology and scientific developments that will bring "a host of divisive new issues before the Supreme Court" within the next decade, including genetic screening and uses of DNA).

12. United States v. Kincade, 379 F.3d 813, 817 (9th Cir. 2004), *cert. denied*, 544 U.S. 924 (2005).

13. *See infra* Part II.

14. *See infra* Parts II, IV.

In this Note, I propose that databanking of individual DNA requires a more complicated analysis than traditional searches under the Fourth Amendment. The practice of taking and storing genetic samples creates an intersection of the Fourth Amendment, informational privacy interests, and various substantive due process rights.[15] I examine a 1977 Supreme Court decision, *Whalen v. Roe*, endorsing a state's storage of private prescription drug information for purposes of analogizing the computerized storage of DNA records and suggesting an informational privacy element.[16] *Whalen's* holding may serve to augment the current jurisprudence surrounding DNA extraction; however, neither rubric—Fourth Amendment nor informational privacy—should be applied mutually exclusively.[17] In fact, unlike searches, DNA databases pose a privacy threat not simply by nature of the extraction but because of the information in the samples that can be accessed again and again. In the proposal, I advocate for a new balancing test to address the informational privacy element of DNA storage and argue for a new judicial analysis. I simultaneously argue that the significance of stringent oversight and national legislation—even the potential creation of a new court and administrative body—cannot be overstated in order to mitigate the "remote possibility"[18] of storing increasing amounts of genetic material that could be used in large-scale practices of abuse and discrimination.[19]

---

15. *See infra* notes 105, 151–54.

16. Whalen v. Roe, 429 U.S. 589 (1977). *See also infra* Part IV.

17. *See infra* Part V. A "special need" to take and store samples of DNA, in the context of fighting a war against terror, might be easily articulated as enhancing national security and preventing crime on a large scale. "In many ways we have already begun to create a 'geneticized' criminal justice system. . . . 'Indirect genetic links between crime and conditions such as alcoholism and antisocial behaviors have been established, and genetic explanations' are currently 'offered to exculpate the accused at trial.'" Elkins, *supra* note 9, at 296 (citing Steven Friedland, *The Criminal Law Implications of the Human Genome Project: Reimagining a Genetically Oriented Criminal Justice System*, 86 KY. L.J. 303, 306 (1997)).

18. *Whalen*, 429 U.S. at 601.

19. While the issue of equal protection under the Fourteenth Amendment is not the subject of this Note, the potential impact of the current anti-terror era bears mentioning. The United States is entering an era where legislation like the USA Patriot Act, *see infra* note 92, while addressing important national security objectives, threatens to encroach with increasing strength on civil liberties of American citizens, and non-citizens as well.

A highly foreseeable legislative development is a statute that denies rights to certain groups of persons based on an anti-terrorism commitment. For example, while strict scrutiny is the standard for evaluating discriminatory laws that target persons based on race, national origin, or alienage, lawmakers could quite easily make the argument that the "strict scrutiny" analysis warrants a new exception when the compelling state interest is preventing terrorism, and treating suspect groups differently would be rationally related to the State's legitimate interest. *See generally* ERWIN CHEMERINSKY, CONSTITUTIONAL LAW PRINCIPLES AND POLICIES 641 (2d ed. 2002). As an example, aliens entering the United States will soon be required to have biometric identifiers in their passports or visas. *See* Enhanced Border Security and Visa Entry Reform Act of 2002 §§ 303–04, 8 U.S.C.

I. BACKGROUND ON DNA DATABASE LEGISLATION

The United States was quick to adopt its own systems of biologically tracking offenders after recognizing the boon to crime fighting that DNA databases afforded Britain.[20] The interests furthered by such an innovation were "undeniably compelling."[21] The theoretical underpinning of DNA storage is the recidivistic nature of violent crimes.[22] A high likelihood exists that a person who has committed violent crimes in the past will continue to do so in the future, and evidence from a crime scene may easily be matched with a profile stored in a database.[23] Congress began a program with the 1994 Violent Crime Control and Law Enforcement Act, authorizing the Federal Bureau of Investigation ("FBI") "to create a national database of DNA samples collected from crime scenes and crime victims, convicted offenders, and unidentified human remains."[24] In 2000, Congress enacted the DNA Backlog Elimination Act of 2000 (the "DNA Act").[25] The DNA Act makes grants to eligible states for use in entering DNA samples from crime scenes and from individuals convicted of qualifying state offenses into a national database system and for increasing the capacity of crime labs owned by state or local governments.[26] In some

§§ 1732–33 (2002). Similarly, when applied to the Fourth Amendment in the context of unreasonable searches and seizures, law enforcement authorities can argue there is a "special needs" justification for keeping DNA files of increasing numbers of individuals in order to keep streets safe from violence and terror. This concept will be discussed at greater length, *infra* Part V.

20. *See infra* notes 21–27 and accompanying text.

21. United States v. Kincade, 379 F.3d 813, 838 (9th Cir. 2004).

22. NIJ SPECIAL REPORT, *supra* note 8, at 9.

23. *Id.*

24. See DNA ANALYSIS BACKLOG ELIMINATION ACT OF 2000, H.R. REP. NO. 106–900 pt. 1, at 8, *discussed in Kincade*, 379 F.3d at 845 (Reinhardt, J., dissenting) [hereinafter DNA ACT HOUSE REPORT]. With the passage of the Anti-Terrorism and Effective Death Penalty Act ("AEDPA"), Pub. L. 104–132, 110 Stat. 1214 (1996), Congress authorized the FBI to "expand CODIS [Combined DNA Index System] to include federal crimes." DNA ACT HOUSE REPORT, *supra* note 24, at 8. For a general overview of the 2000 Act, see Richard P. Shafer, Annotation, *Validity, Construction, and Application of DNA Analysis Backlog Elimination Act of 2000*, 187 A.L.R. FED. 373 (2003).

25. DNA Analysis Backlog Elimination Act of 2000, Pub. L. No. 106–546, 114 Stat. 2726 (codified at 42 U.S.C. § 14135a(a)(2) (2000)) [hereinafter DNA Act]. The purposes of the DNA Act also include eliminating DNA backlogs and using DNA to protect innocent individuals wrongly convicted of crimes. *Id.* These issues are not the subject of this Note.

26. See *id.*, stating the purpose of the Act is "[t]o make grants to States for carrying out DNA analyses for use in the Combined DNA Index System of the Federal Bureau of Investigation, to provide for the collection and analysis of DNA samples from certain violent and sexual offenders for use in such system, and for other purposes."

Pursuant to the DNA Act, individuals who have been convicted of certain federal crimes and who are incarcerated, or on parole, probation or supervised release must provide federal authorities with a DNA sample, defined as "a tissue, fluid, or other bodily sample . . . on which [a]n . . . analysis of th[at sample's] deoxyribonucleic acid (DNA) identification information" can be performed. 42 U.S.C.

cases, databases even contain profiles of arrestees, who were convicted of no crime whatsoever.[27] Requirements for DNA storage vary from state to state.[28]

The DNA Act has enabled a streamlined process of tracking DNA profiles on local, state, and national levels.[29] Once an individual's DNA profile has been produced (either by mandatory extraction or from crime scene evidence), the resulting record is entered into the FBI Combined

---

§ 14135a(a)(1)–(2), (c)(1)–(2) (2000). The Federal Bureau of Investigation ("FBI") considers DNA information derived from blood samples to be more reliable than that obtained from other sources (in part because blood is easier to test and to preserve than hair, saliva, or skin cells). *See generally* Nancy Beatty Gregoire, *Federal Probation Joins the World of DNA Collection*, 66 FED. PROBATION 30 (2002). As such, FBI guidelines require those in federal custody and subject to the DNA Act to submit to compulsory blood sampling. *Id.* at 31, *cited in Kincade*, 379 F.3d at 817. Failure to cooperate in the collection of the DNA sample is a class A misdemeanor, punishable by up to one year's imprisonment and a fine of as much as $100,000. 42 U.S.C. § 14135a(a)(5); 18 U.S.C. §§ 3571, 3581 (2000).

Although the list of qualifying offenses in 2000 was quite narrow, including arson, voluntary manslaughter, and murder, the scope has proliferated to reach numerous federal crimes, even including "willfully injur[ing] or commit[ting] any depredation against any property of the United States." *Kincade*, 379 F.3d at 846 (Reinhardt, J., dissenting) (quoting 18 U.S.C. § 1361 (2000)). This includes spray painting graffiti on a government building or perhaps tearing apart a $1 bill. *Id.* "Recent legislation in several states has authorized the federal government to store and access DNA profiles of individuals who have been convicted of run-of-the-mill non-violent crimes such as felonious possession of food stamps," *id.* at 848 (citing Br. of Amicus Curiae Public Defender Service for the District of Columbia, at 6 (citing ALA. CODE §§ 36-18-24, 13A-9-91 (2003))).

Judge Reinhardt notes that, "[w]ith nearly 6.9 million individuals under some form of correctional supervision in recent years, CODIS has the immediate potential for exponential growth." *Kincade*, 379 F.3d at 848 (Reinhardt, J., dissenting) (citations omitted). Additionally, it is apparent that minorities are disproportionately represented in these correctional systems. *Id.*

27. *Kincade*, 379 F.3d at 848 (Reinhardt, J., dissenting) (citing Br. of Amicus Curiae Public Defender Service for the District of Columbia, at 7 (citing LA. REV. STAT. ANN. § 15:609(A) (West Supp. 2003); TEX. GOV'T CODE ANN § 411.1471(a)(2) (West 2003); Va. St. § 19.2-310.2:1 (2003))). Of note, California recently amended its laws with Proposition 69, expanding its DNA database to include samples from arrestees. See *infra* note 161.

28. In 1989, Virginia was the first state to set up a DNA database in the United States, with a law requiring convicted sex offenders to give blood samples. Allison Puri, Note, *An International DNA Database: Balancing Hope, Privacy, and Scientific Error*, 24 B.C. INT'L & COMP. L. REV. 341, 357–58 (2001); *see also* Mark Stencel & Carlos Sanchez, *DNA Database Leads Police to Suspect; Genetic Material used for First Time in Virginia to Bring Charge*, WASH. POST., Oct. 19, 1993, at B1. Virginia quickly chose to broaden the scope of offenders so as to include samples from convicted sex offenders, nonviolent felons, and even juveniles. *Id.*; *see also* Julia Scheeres, *Fears About DNA Testing Proposal*, WIRED NEWS, Mar. 31, 2003, http://www.wired.com/news/politics/0,1283,58270,00.html. In 2003, Virginia began collecting DNA samples from anyone charged with a violent felony. Maria Glod, *Va. to Begin Taking DNA After Arrests for Felonies; Prosecutors, Rights Activists Split on Database Expansion*, WASH. POST., Jan. 1, 2003, at B1.

All 50 U.S. states currently allow extraction and storage for inclusion in databases of criminal DNA. GENETIC PRIVACY, *supra* note 1. Every state now requires DNA samples from convicted sex offenders, and some, such as Virginia, require samples from some or all felons. *Id.* Each law maintains different regulations for the length of time samples will remain in the database. *Id.* At the national database level, samples are retained indefinitely. *Id.*

29. NIJ SPECIAL REPORT, *supra* note 8, at 9–10.

DNA Index System ("CODIS").[30] CODIS is a massive centrally-managed database linking DNA profiles culled from federal, state, and local DNA collection programs, in addition to profiles from crime-scene evidence or unidentified remains.[31] As of September 2005, CODIS contained DNA profiles drawn from 2,763,191 offenders and 119,782 crime scenes.[32]

Where law enforcement officers already have a suspect identified, the sample of that individual's DNA can be compared with evidence from the crime scene.[33] Otherwise, CODIS functions in two primary capacities to aid investigations. Where no suspect has been identified, evidence from a crime scene can be compared with DNA profiles in DNA databases and matched to a perpetrator in the database.[34] Additionally, crime scene evidence that is unidentified can be entered into the database for purposes of future matches.[35]

II. THE 2004 *KINCADE* DECISION AND HISTORY

Since the inception of DNA databases and the use of genetic material to solve crimes, courts have grappled with the constitutional issues raised by forcing offenders to submit samples for storage in a state or national database.[36] Courts have uniformly considered sample extraction to be governed by the Fourth Amendment and have agreed that the taking of a blood sample amounts to a "search," which is barred by the Fourth Amendment absent probable cause.[37] Additional complications arise when the requirement of a blood sample is a condition of parole or supervised release, at a time when an offender has completed a prison term.[38]

---

30. *Id.* at 10.

31. *Id.* at 9.

32. FED. BUREAU OF INVESTIGATION, NDIS STATISTICS, http://www.fbi.gov/hq/lab/codis/clickmap.htm, *cited in Kincade*, 379 F.3d at 819.

33. STATEMENT OF THE WHITE HOUSE: ADVANCING JUSTICE THROUGH THE USE OF DNA TECHNOLOGY 1 (March 2003), *available at* http://www.whitehouse.gov/infocus/justice/dna_initiative_policy_book.pdf [hereinafter WHITE HOUSE DNA STATEMENT].

34. *Id.*

35. *Id.*

36. For a discussion of the constitutionality challenges to the DNA Act on Fourth Amendment grounds, see Shafer, *supra* note 24.

37. U.S. CONST. amend. IV. *See also* Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 616 (1989) (bodily intrusion resulting from extracting a blood sample constitutes a search under the Fourth Amendment). Judge Hawkins noted in a solo *Kincade* dissent that the physical intrusion of taking a blood sample should not be overlooked: "no one is required to submit to 'intrusions beyond the body's surface' absent a 'clear indication' that the desired evidence would be found by such a search." *Kincade*, 379 F.3d at 875 (Hawkins, J., dissenting) (quoting Schmerber v. California, 384 U.S. 757, 769–70 (1966)).

38. This issue was the crux of the *Kincade* appeal. The federal DNA Act makes it a crime to

The U.S. Supreme Court instructs that withdrawing blood normally requires a warrant.[39] In order to determine whether a DNA collection statute is constitutionally sound, courts have evaluated the reasonableness of the search.[40] The reasonableness analysis in these cases has often involved a balancing of the potential privacy intrusion on the individual suspect against the government's interest in using the extracted material to solve past or future crimes.[41] The Supreme Court has endorsed warrantless, suspicionless searches when they advance "special needs" that go "beyond the normal need for law enforcement."[42] The Second, Seventh, and Tenth Circuits, along with federal district courts and at least two state supreme courts, have upheld DNA collection statutes under this "special needs" analysis.[43] The Fourth and Fifth Circuits, a Seventh Circuit

---

refuse conditions of parole requiring a person to submit a blood sample for storage and future use: "An individual from whom the collection of a DNA sample is authorized under this subsection who fails to cooperate in the collection of that sample shall be—(A) guilty of a class A misdemeanor; and (B) punished in accordance with title 18 [United States Code]." DNA Act, 42 U.S.C. § 14135a(a)(5) (2000). However, Mr. Kincade and others have objected on constitutional grounds to such a "search" absent suspicion and probable cause. United States v. Kincade, 379 F.3d 813, 820–21 (9th Cir. 2004). The purpose of the requirement is a future crime-fighting tool. However, when an individual on supervised release is asked for a sample, he has already completed his prison term, or colloquially, has done his time. Thus, no probable cause may exist to warrant a "search" under the Fourth Amendment. "Supervised release" replaced federal "parole" with the Sentencing Reform Act of 1984. Pub. L. No. 98-473, § 212(a)(2), 98 Stat. 1987 (1984). As opposed to parole, supervised release follows a term of imprisonment instead of shortening it. *Id.*

39. *Schmerber*, 384 U.S. at 770. In this case, a suspect was given an involuntary blood test in the hospital following a car accident in order to determine whether he was driving while intoxicated.

40. The tricky aspect of evaluating reasonableness of searches in the context of DNA for storage and future use is that reasonable suspicion for the search is not a factor. Indeed, "[t]he very idea of establishing a data bank refutes the possibility of establishing individualized suspicion because the collection of the blood samples is designed to solve future cases for which no present suspicion can exist." Jones v. Murray, 962 F.2d 302, 305 (4th Cir. 1992) (holding that the taking and storing of blood from convicted felons under a Virginia statute does not violate the Fourth Amendment).

41. Landry v. Attorney Gen., 709 N.E.2d 1085, 1091 (Mass. 1999) (overturning the lower court decision, and holding that "the high government interest in a particularly reliable form of identification outweighs the minimal intrusion of a pin prick").

42. New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring). *See also* Ferguson v. City of Charleston, 532 U.S. 67, 79 (2001) (reasoning that no programmatic suspicionless search is reasonable unless the special need is "divorced from the State's general interest in law enforcement"); City of Indianapolis v. Edmond, 531 U.S. 32, 37 (2000) (acknowledging that one of the limited exceptions to the accepted rule requiring suspicion for a search was when the search was justified by "special needs, beyond the normal need for law enforcement").

The *Kincade* court noted three general "regimes" of searches that are not subject to the usual warrant and probable cause requirements, one of which is "special needs." *Kincade*, 379 F.3d at 823. Another regime is "exempted areas," including searches at the border, *see* United States v. Ramsey, 431 U.S. 606, 616 (1977); in prisons, *see* Hudson v. Palmer, 468 U.S. 517, 526 (1983); and airports and entrances to government buildings, *see* Chandler v. Miller, 520 U.S. 305, 323 (1997). *Kincade*, 379 F.3d at 822 nn.16–18. The final category is "administrative searches," and includes inspections of "closely-regulated businesses." *Id.* at 823.

43. *Kincade*, 379 F.3d at 830. The Ninth Circuit referenced several court opinions falling into the

judge, several federal district courts, and state courts have approved compulsory DNA profiling using a broad evaluation of the totality of the circumstances.[44]

In August 2004, the Ninth Circuit Court of Appeals entered the dialogue by validating extraction of DNA for convicted felons on release.[45] Overturning its previous panel decision, the court held en banc in a tight six-five decision that the requirement under the DNA Act that certain federal offenders on parole, probation, or supervised release submit DNA samples for profiling, in absence of individualized suspicion that they had committed additional crimes, was reasonable and did not violate the Fourth Amendment.[46] Reaffirming a 1995 decision upholding the constitutionality of a state DNA collection statute,[47] the Ninth Circuit held that a totality of the circumstances analysis comported with Supreme

---

"special needs" analytical framework. *See, e.g.*, Green v. Berge, 354 F.3d 675, 679 (7th Cir. 2004); United States v. Kimler, 335 F.3d 1132, 1146 (10th Cir. 2003); Roe v. Marcotte, 193 F.3d 72, 79–82 (2d Cir. 1999); Vore v. U.S. Dep't of Justice, 281 F. Supp. 2d 1129, 1133–35 (D. Ariz. 2003).

44. *Kincade*, 379 F.3d at 831. The Ninth Circuit referenced several court opinions falling into the "totality of the circumstances" analytical framework. *See, e.g.*, *Green*, 354 F.3d at 680–81 (7th Cir. 2004) (Easterbrook, J., concurring); Groceman v. U.S. Dep't of Justice, 354 F.3d 411, 413–14 (5th Cir. 2004) (per curiam); Velasquez v. Woods, 329 F.3d 420, 421 (5th Cir. 2003) (per curiam); Jones v. Murray, 962 F.2d 302, 306–07 (4th Cir. 1992).

45. In *Kincade*, the Ninth Circuit became the sixth federal court of appeals to approve forced DNA extraction for convicted felons or parolees. *See supra* note 43; *see generally* Maura Dolan & Andrew Blankstein, *Parolee DNA Testing Okd; Federal Convicts Can be Forced to Provide Blood Samples, an Appeals Court Rules. Critics See a Threat to Privacy*, L.A. TIMES, Aug. 19, 2004, at B1; Jeff Chorney, *As 9th Circuit Oks DNA Profiling, Dissent Cries Big Brother*, THE RECORDER, Aug. 19, 2004, (News), at 1.

Of note, *United States v. Miles* is the exceptional case. 228 F. Supp.2d 1130 (E.D. Cal. 2002). The *Miles* court found the DNA Act violative of the Fourth Amendment when a defendant who had been convicted thirty years prior of a qualifying offense was required to submit a sample absent any individualized suspicion. *Id.*

46. *Kincade*, 379 F.3d 813. In July of 1993, Thomas Cameron Kincade robbed a bank with a firearm in violation of 18 U.S.C. §§ 2113(a), (d), 924(c)(1). *Id.* at 820. After a plea of guilty, Kincade "was sentenced to 97 months of imprisonment, followed by three years' supervised release." *Id.* In March of 2002, Kincade refused his probation officer's request for him to submit a blood sample pursuant to the DNA Act. *Id.* As a result, he was sentenced to four months' imprisonment and two years' supervised release for violating terms of his supervised release. *Id.* at 821. Kincade appealed after the U.S. District Court for the Central District of California rejected his constitutional claim. *Id.* Pursuant to the Fourth Amendment,

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

47. Rise v. Oregon, 59 F.3d 1556 (9th Cir. 1995) (upholding the constitutionality of a state DNA collection statute by applying a pure totality of the circumstances analysis, considering factors such as a reduced expectation of privacy on the part of persons who commit crimes, and the public interest in preventing those persons from repeating their crimes).

Court precedent as well as requirements under the Fourth Amendment.[48] Emphasizing the conditional releasees' substantially diminished expectations of privacy, the "minimal intrusion" apparent in blood sampling, and the "monumental" government interest, the court concluded that compulsory DNA profiling is reasonable under the totality of the circumstances.[49]

Judge Stephen Reinhardt, joined by two other judges, offered a vigorous dissent to the plurality's broad analysis.[50] With Orwellian undertones, he raised doubts about the narrow application of DNA testing to a convicted felon on supervised release:

> [U]nder the rationales [the plurality] espouse[s] . . . all Americans will be at risk, sooner rather than later, of having our DNA samples permanently placed on file in federal cyberspace, and perhaps even worse, of being subjected to various other governmental programs providing for suspicionless searches conducted for law enforcement purposes.[51]

Judge Reinhardt's primary concern centered on the plurality's sweeping approval of a search designed to produce and maintain criminal evidence absent any scintilla of individualized suspicion.[52] In addition, he noted that the bureaucracy in charge of storing and overseeing such collected information "[was] poorly regulated and susceptible to abuse. . . . exposing individuals to a series of harms, increasing their vulnerability

---

48. *Kincade*, 379 F.3d at 832. The Ninth Circuit emphasized the Supreme Court's holding in *United States v. Knights*, 534 U.S. 112 (2001), which authorized a warrantless search of a probationer's home based on a reasonable hunch that the probationer was involved in crimes against Pacific Gas & Electric ("PG&E"). *Kincade*, 379 F.3d at 827–32. By analogy, the Ninth Circuit reasoned that the Supreme Court's use of a totality of the circumstances balancing test of the probationer's interest in privacy against the state's interest in searching his home without a warrant should apply likewise to Mr. Kincade. *Id.* at 827–28.

49. *Kincade*, 379 F.3d at 839. Emphasizing the benefits to society of this practice, the plurality opinion stated:

> As a deterrent, DNA profiling can help to steer conditional releasees toward law-abiding lives as productive members of our society, fostering the rehabilitative goal of our systems of conditional release. Such profiling likewise helps protect the society into which offenders are conditionally released by reducing crime attributable to the operation of limited release programs like probation and parole. And by laying a foundation for solving those crimes that are not successfully deterred by the collection of DNA profiles, the DNA Act both provides a means to monitor individuals' compliance with the terms of their release and helps minimize the pain and suffering recidivist offenders sow in our communities.

Id. at 839 (citations omitted).

50. *Kincade*, 379 F.3d at 842 (Reinhardt, J., dissenting).

51. *Id.*

52. *Id.* at 843.

and decreasing the degree of power that they exercise over their lives."[53] It was the "opaque" use of the totality of the circumstances test to sweep away the traditional Fourth Amendment requirement of some level of suspicion that Reinhardt concluded was especially troubling.[54]

Noting the plurality's deference to the reduced expectation of privacy of a parolee or releasee, Judge Reinhardt raised the possibility that the category may be extended by analogy to other individuals who are not felons.[55] For example, "attendees of public high schools or universities, persons seeking to obtain drivers' licenses, applicants for federal employment, or persons requiring any form of federal identification" all experience a reduction in expectation of privacy.[56] In short, Reinhardt admonished that by employing a standard that "imposes no significant limits on arbitrary and invasive government actions," the plurality "opens the door to multifarious law enforcement programs involving suspicionless searches."[57]

The Supreme Court has drawn a line between searches where there is a strong government interest, accompanied by minimal intrusion on the subject, and searches where there is only a general law enforcement interest.[58] Specifically, the Court has upheld programs requiring student athletes to submit to random drug testing where there is no reporting to law enforcement officials.[59] The Court has upheld suspicionless border

---

53. *Id.* (quoting Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1105 (2002) [hereinafter Solove, *Digital Dossiers*]).

54. *Id.* Judge Reinhardt noted the thinness of the plurality analysis:

> The "totality" of the circumstances relied upon by the plurality is as follows: Those who commit crimes have reduced expectations of privacy and, because the forcible extraction of blood is a constitutionally insignificant invasion of privacy, and the weight of the government interest in DNA profiling "is monumental," suspicionless searches are constitutionally reasonable.

Id. (citations omitted). Los Angeles Supervising Deputy Federal Public Defender Monica Knox acknowledged that the U.S. Supreme Court has never agreed that a totality of the circumstances argument overrides the "reasonable suspicion" requirement of Fourth Amendment searches. Chorney, *supra* note 45.

55. *Kincade*, 379 F.3d at 844 (Reinhardt, J., dissenting).

56. *Id.*

57. *Id.* Reinhardt notes that the CODIS database's rapid expansion represents an

> alarming trend whereby the privacy and dignity of our citizens [are] being whittled away by [ ] imperceptible steps. Taken individually, each step may be of little consequence. But when viewed as a whole, there begins to emerge a society quite unlike any we have seen—society in which government may intrude into the secret regions of man's life at will.

Id. at 851 (quoting Osborn v. United States, 385 U.S. 323, 343 (1966) (Douglas, J., dissenting)).

58. Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656 (1989); Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602 (1989) (articulating balancing test to identify special needs of the government).

59. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995). *See also* Bd. of Educ. of Indep. Sch.

checkpoints put in place to intercept illegal aliens, based on a unique government interest in border patrol.[60] Similarly, the Court has upheld suspicionless roadside sobriety checkpoints, based on the immediate bodily threat caused by drunk drivers, and a corresponding higher-than-normal law enforcement interest.[61] A legitimate government interest also outweighs employee privacy concerns related to mandatory drug and alcohol testing in regulated industries such as railroads.[62] However, the Court has stopped short of allowing roadside searches justified only by a generalized possibility that interrogation and inspection at a given checkpoint may reveal that any given motorist may have committed some yet-unforeseen crime.[63] The Court has similarly invalidated a public hospital's non-consensual drug testing of maternity patients, based on the possibility of a positive result.[64]

In spite of what the *Kincade* court might refer to as close cases under the Supreme Court, Reinhardt declared that "[n]ever once in over two hundred years of history has the Supreme Court approved of a suspicionless search designed to produce ordinary evidence of criminal wrongdoing for use by the police."[65] Thus, noted Reinhardt, the *Kincade* holding contravenes precedent with its broad "totality of the circumstances" catchall.[66] The primary purpose of searches conducted under the DNA Act is to "'help law enforcement solve unresolved and future cases.'"[67] The taking of samples under these auspices amounts to a suspicionless search for ordinary law enforcement interests—fighting of past and future crimes.[68] Reinhardt's dissent thus serves to caution that the

---

Dist. No. 92 v. Earls, 536 U.S. 822 (2002) (holding that urine testing of students for extracurricular activities to prevent health and safety risks from drug use were valid, so long as the results were not turned over to any law enforcement authority).

60. United States v. Martinez-Fuerte, 428 U.S. 543 (1976).

61. Mich. Dep't of State Police v. Sitz, 496 U.S. 444 (1990).

62. *Skinner*, 489 U.S. 602.

63. City of Indianapolis v. Edmond, 531 U.S. 32 (2000).

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

65. United States v. Kincade, 379 F.3d 813, 854 (9th Cir. 2004) (Reinhardt, J., dissenting). *See also Edmond*, 531 U.S. at 41 (The Court has "never approved [a general program of suspicionless seizures] whose primary purpose was to detect evidence of ordinary criminal wrongdoing."). Furthermore, there exists a danger that justifying suspicionless searches by a general law enforcement interest would allow such intrusions to become "a routine part of American life." *Id.* at 42.

66. "[The plurality] adopt[s] a sweeping totality the circumstances test . . . blatantly eviscerating the constitutional requirement of individualized suspicion for law enforcement searches." *Kincade*, 379 F.3d at 843 n.1 (Reinhardt, J. dissenting).

67. *Id.* at 855.

68. In fact, the Department of Justice maintained before Congress that "one of the underlying concepts behind CODIS is to create a database of convicted offender profiles and use it to solve crimes for which there are no suspects." DNA ACT HOUSE REPORT, *supra* note 24, at 27 (2000), *quoted in*

plurality's foray into "monumental" law enforcement interests based on a "totality of the circumstances" analysis "dismantles the structural protections that lie at the core of the Fourth Amendment,"[69] widening the path to ever-increasing suspicionless searches that may serve some vague law enforcement utility.

III. CIVIL LIBERTIES CONCERNS

In its Brief of Amicus Curiae ("EPIC Brief") submitted to the Ninth Circuit before the en banc rehearing of *Kincade*, the Electronic Privacy Information Center ("EPIC")[70] cautioned against the many adverse consequences of allowing forced DNA extraction absent individualized suspicion.[71] DNA databases may vastly expand in the future to include DNA from the general public.[72] I will address each of these concerns in turn, in an effort to amplify the arguments offered in Judge Reinhardt's dissent and to provide the background for my analysis of mass computerized DNA storage, a hybrid between a "search" and invasion of informational and bodily privacy.[73]

Kincade, 379 F.3d at 856 (Reinhardt, J., dissenting). *See also* 146 CONG. REC. S11,647 (daily ed. Dec. 6, 2000) (statement of Sen. Leahy) (purpose of DNA profiling within CODIS is to "solve crimes and prevent further crimes").

69. *Kincade*, 379 F.3d at 870 (Reinhardt, J., dissenting).

70. The Electronic Privacy Information Center ("EPIC"), established in 1994, is a public interest research center based in Washington, D.C., created "to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment and constitutional values." EPIC Home Page, http://www.epic.org (follow "What is EPIC?" hyperlink under "About EPIC").

71. Brief of Amicus Curiae Electronic Privacy Information Center, United States v. Kincade, 379 F.3d 813 (9th Cir. 2004) (No. 02-50380) [hereinafter EPIC Brief].

72. NAT'L COMM'N ON THE FUTURE OF DNA EVIDENCE, NAT'L INST. OF JUSTICE, U.S. DEP'T OF JUSTICE, THE FUTURE OF FORENSIC DNA TESTING: PREDICTIONS OF THE RESEARCH AND DEVELOPMENT WORKING GROUP 35–36 (2000), *available at* http://www.ncjrs.org/pdffiles1/nij/183697.pdf [hereinafter FUTURE OF FORENSIC DNA TESTING]. According to the report,

> Inevitably, there will be the increasing possibility of broadening the database to include the general public. There would be many advantages, such as identification of persons or body parts after accidents, or discovery of kidnapped or lost people. At the same time, the risk to individual privacy would be enhanced and protection of anonymity would be harder.

Id., *quoted in* EPIC Brief, *supra* note 71, at 5.

73. As discussed *infra*, there are many reasons to be wary of mass computerized storage of any private information, let alone individual DNA samples. The EPIC Brief argues that the forced sampling of DNA under the current federal legislation is violative of the Fourth Amendment. EPIC Brief, *supra* note 71, at 1. The EPIC Brief emphasizes the slippery slope ramifications of DNA databanking—specifically, that a DNA sample offers "insights into many intimate aspects of a person and their families including susceptibility to particular diseases, legitimacy of birth, and perhaps predispositions to certain behaviors and sexual orientation. This increases the potential for genetic discrimination by government, insurers, employers, schools, banks, and others." EPIC Brief, *supra* note 71, at 1 (quoting U.S. Dep't of Energy Office of Science et al., *DNA Forensics*, Human Genome Project Information, http://www.orvil.gov/sci/techresources/Human_Genome/elsi/forensics.shtml).

A. The information contained in a DNA sample is substantial and reveals private genetic data

DNA samples offer insight into unique aspects of a person as well as that person's family, including susceptibility to particular diseases, predictive health, and other information that is highly personal in nature.[74] The information available in a DNA sample may even be found to elucidate certain behaviors and sexual orientation, and even predisposition to violence or crime.[75] Indeed, "the quest for the criminal gene holds obvious attractions for the forces of law and order."[76] The availability of

---

74. "In an age of biotechnology and computers, we are all but a needle-stick away from disclosing hereditary-disease susceptibilities, familial relationships and identifying information." Kimmelman, *supra* note 5. "Anyone who values privacy should therefore be concerned that US law-enforcement agencies are amassing ever larger portions of the general population's DNA while neglecting to implement measures that would protect the privacy and presumptive innocence of citizens." *Id.*

The FBI currently employs a short tandem repeat ("STR") technology to create profiles for the database. NIJ SPECIAL REPORT, *supra* note 8, at 6. STR technology is used to evaluate thirteen markers or loci within a cell's nucleus, and these loci are located within "junk DNA," or DNA with no known function for trait coding. *Id.*

75. *See* GENETIC PRIVACY, *supra* note 1. The link between genes and behavior is a highly controversial subject among genetic researchers. *Id.* Despite this, however,

> [r]esearchers have made claims that genes influence such traits as alcoholism, homosexuality, thrill seeking, nurturing, and tendencies toward violent criminal behavior. These claims are based on indications that some behaviors are species-specific, can persist from generation to generation, and can change as a result of brain injury or other biological alteration . . . . [I]t is possible that someone who is found to have a predisposition to violence might receive a harsher criminal sentence for a non-violent offense because of a presumption that he poses a danger to society due to his genetic make-up.

Id. See also Interview by Leslie Glass with Dr. Lawrence Kobilinsky, DNA Expert, *Should We DNA Type Anyone Who's Arrested?*, http://www.mystery-book.com/dna_testing.html (last visited Oct. 21, 2005). According to Dr. Lawrence Kobilinsky, forensic scientist and Associate Provost at John Jay College of Criminal Justice, "a DNA profile can show a lot about personality, too, and possibly even predict the potential for violent, antisocial behaviors. It's possible DNA could also be used, or abused, as a predictor of behavior." *Id.*

76. John Lettice, *Report Warns of Dangers of UK's DNA Database*, THE REGISTER, Jan. 13, 2005, *available at* http://www.theregister.co.uk/2005/01/13/genewatch_dna_database/. Studies have often claimed to find "genetic links to traits such as homosexuality, aggression, depression or addictive personality. . . ." *Id.*; *see also* Kimmelman, *supra* note 5 (cautioning that "tissue repositories created by databanks would provide genetics researchers with congenial waters in which to trawl for genes thought to be involved in criminal behavior"). Even more troubling, "Alabama's databanking law brushes perilously close to this by authorizing release of anonymous DNA population data collected by law-enforcement authorities to 'assist in other humanitarian endeavors including, but not limited to, educational research or medical research or development.'" Kimmelman, *supra* note 5. These concerns could be even further exacerbated when considering the possible privatization of DNA databases. *See, e.g.*, Philip Johnston, *DNA Crime Files May be Sold Off*, THE DAILY TELEGRAPH (London), July 18, 2003, at 11 (the United Kingdom's national DNA database "could end up in the private sector under the Government's plans to sell off the Home Office Forensic Science Service (FSS)").

For a discussion of an innovative approach to predicting criminality, see Emily Bazelon, *Sentencing by the Numbers*, N.Y. TIMES, Jan. 2, 2005, § 6 (Magazine) at 18. The article discusses the

such sensitive information increases the potential for genetic discrimination by the government, insurers, employers, schools, banks, and others.[77] The Council on Responsible Genetics has already documented instances of employers and insurers using results of genetic tests to decide whether to employ or insure an individual, for example, if the individual possesses genes associated with health risks or predispositions.[78] Moreover, because genetic information is shared with biological relatives, an individual's profile might indirectly implicate a relative in an offense.[79]

Commonwealth of Virgina's new approach to fighting crime. The State now encourages judges to sentence nonviolent offenders "the way insurance agents write policies, based on a short list of factors with a proven relationship to future risk." *Id.* A study that tracked 1,500 nonviolent offenders for three years after their release from prison spawned this unique policy. *Id.* The state sentencing commissioner devised a variety of factors, such as age, gender, and employment status, to discern risk assessment of defendants. *Id.* If the defendant scores a thirty-five or less on this scale, the judge may recommend a sanction other than prison, such as probation or house arrest. *Id.* Such a policy indicates that state law enforcement agencies, when faced with similar budget crunches, might look to alternatives to fight crime faster and with less expense. Use of genetic factors might well top the list.

77. Wendy McGoodwin, head of the Council for Responsible Genetics in Cambridge, Massachusetts, cautions that the potential for DNA databases to be abused:

> Our organization has documented numerous examples of genetic discrimination where healthy individuals have either lost their insurance or their jobs on the basis of predictive genetic information. Doctors are now able to test for hundreds of gene mutations that may put people at risk for future disease—diseases such as cystic fibrosis or sickle cell anemia. Now it's very important for your doctor to have that information but it can be very dangerous if that information falls into the wrong hands.

Beth Anne Bowser, *Strands of Justice*, The NewsHour with Jim Lehrer Transcript (July 10, 1998), http://pbs.org/newshour/bb/law/july-dec98/dna_7-10.html [hereinafter *NewsHour Transcript*]. Moreover, increasing numbers of groups might claim an interest in the secrets DNA reveals, in addition to scientists, employers and insurers. Dr. Philip Reilly, executive director of the Shriver Center for Mental Retardation in Massachusetts, who has studied DNA data banking, has other concerns:

> Let's say they find a gene for learning disabilities in kids. Someone might argue that school systems have a right to know this information in order to help the child. But someone else might argue that if the school system knows this about a child, it will simply give up on him.

Nathan Cobb, *The End of Privacy; Computers now Track our Purchases, Conversations, Comings and Goings. They Also Threaten to Expose What Little Remains of our Private Lives*, BOSTON GLOBE, Apr. 26, 1992, Magazine, at 16. Yet another concern raised by data banking is genetic research focusing on ethnic or racial groups. For example, Howard University plans to create a database of African-American DNA, deriving from 25,000 people over a five-year period, in efforts to study genetic diseases common to African-Americans. *See* Gaia Bernstein, *Accommodating Technological Innovation: Identity, Genetic Testing and the Internet*, 57 VAND. L. REV. 965, 990–91 (2004). "Unlike regular medical information, genetic information renders individuals as innately different, thereby becoming a dangerous tool in the hands of those seeking to discriminate and stigmatize." *Id.* at 991.

78. CRG POSITION PAPER, *supra* note 9. "As these tests become simpler to administer and their use expands, the CRG strongly believes that employers and insurers will continue to use genetic information in a discriminatory manner and that a growing number of people will be stigmatized on the basis of their genetic makeup." *Id.*

79. For example, a publicized United Kingdom "breakthrough" occurred in 2004 when a Florida company claimed to be able to ascertain a suspect's broad ancestry. Based on his DNA, the company

B. Potential non-law enforcement purposes for reanalyzing DNA could beget misuse and abuse of samples

All states currently maintain some type of DNA database and policies to guard the databases, but there are no guidelines or standards for handling the DNA sample after it is added to the database.[80] There is no universal standard for expungement of a DNA record or sample after a conviction is overturned.[81] The resulting danger is that DNA could become available to unauthorized parties or otherwise be used in ways that would disclose information that ought to remain confidential. For example, scientists may start to request access to what might be considered a windfall of DNA data for their research. Scientists could argue for the potential benefit to humanity in studying gene patterns among those persons with a propensity for criminal activity. According to Barry Scheck of The Innocence Project at the Benjamin N. Cardozo School of Law,

> I can easily imagine, unless they correct this legislation, that somebody will come along someday very soon and say look, I have a law enforcement purpose—I want to get access to the DNA you took from all these convicted sex offenders, and I want to do some screening on it because I think I can find a gene that shows the people committing sexual assaults, or I can find a gene that's related to violent behavior or homicidal behavior . . . I want to experiment with it.[82]

---

determined him to be from the Caribbean. *See* Lettice, *supra* note 76. The fruits of DNA research and technology are truly in nascent stages. Scientist Paul Hebert, a zoologist at the University of Guelph in Ontario, predicts that in ten years, a DNA barcode scanner will be "so simple to use that anyone can identify any organism they encounter." John Roach, *Handheld DNA Scanners to ID Species Instantly?*, NATIONAL GEOGRAPHIC NEWS, Jan. 26, 2005, http://news.nationalgeographic.com/news/2005/01/0126_050126_dnabarcode.html. Scientists are currently collaborating on DNA bar-coding science and aiming to create a bar code database for Earth's estimated ten million species. *Id.* While this technology is designed to expedite discovery of new species and analyze diseases of various organisms, the application could easily take hold in law enforcement for analysis of human tissue. *See also* Nicholas Wade, *A Species in a Second: Promise of DNA "Bar Code*," N.Y. TIMES, Dec. 14, 2004, at F1.

80. FUTURE OF FORENSIC DNA TESTING, *supra* note 72, at 36.

81. *See* Michelle Hibbert, *DNA Databanks: Law Enforcement's Greatest Surveillance Tool?*, 34 WAKE FOREST L. REV. 767, 807–812 (1999). Saving DNA permits retesting and inclusion of additional loci, particularly newly discovered markers. FUTURE OF FORENSIC DNA TESTING, *supra* note 72, at 36.

82. *NewsHour Transcript*, *supra* note 77. In the same program, the director of the Virginia Division of Forensic Science, Dr. Paul Ferrara, suggested that the way to avoid abuse is to have laws to prevent it: "You do it by regulation; you do it by statute; you do it by imbuing on people ethical, responsible behavior." *Id. See also* Shaila K. Dewan, *Police Try Extending Use of DNA Tests to More Crimes*, N.Y. TIMES, Oct. 26, 2004, at B1. "Dr. Paul Ferrara . . . said that in a study of the [Virginia]

The possibility for such misuse of DNA is very real. In fact, in March 2003, then Attorney General John Ashcroft announced an initiative seeking $1 billion over five years for the purpose of "realiz[ing] the full potential of DNA technology to solve crime and protect the innocent."[83] Currently no law exists to punish violations for obtaining medical information for wrongful purposes, such as experimenting with genetic traits or characteristics.[84] Furthermore, there are no universal policies protecting security of DNA databases or mandating audits and accountability.[85]

Other countries, such as Canada and Australia, allow individuals such as crime victims, witnesses, and volunteers of DNA to limit the use of a provided sample.[86] In addition, these individuals, or even a crime suspect,

---

database's first 1,000 hits, there were 244 matches in sexual assault cases. Fifty-four of those suspects were in the database because of prior burglary convictions, compared to just thirty-five with prior drug convictions." *Id.*

83. *See* WHITE HOUSE DNA STATEMENT, *supra* note 33, at 2. *See also* Rosen, *supra* note 5. The initiative announced by Ashcroft seeks to expand the CODIS database. *Id.* The Bush administration is in favor of providing the FBI with unfettered access to samples within state DNA databases, including the DNA material from arrestees in some states. *Id.*

84. COMM. ON DNA TECH. IN FORENSIC SCI., DNA TECHNOLOGY IN FORENSIC SCIENCE 122 (Nat'l Research Council ed., 1992), *cited in* EPIC Brief, *supra* note 71, at 10.

85. GENETIC PRIVACY, *supra* note 1. "[C]omplex and multi-layered security arrangements" should be put in place in order to protect privacy of the individual samples. *Id.* These databases "require appropriate safeguards for storage of physical samples, database security for DNA profile databases, and security mechanisms to protect the links between the two." *Id.*

86. See DNA Identification Act, 1998 S.C., ch. 37, §§ 6(6), 8.1, 9(2) (Can.), *available at* http://laws.justice.gc.ca/en/D-3.8/49333.html. The text reads as follows: "No person who receives a DNA profile for entry in the DNA data bank shall use it or allow it to be used other than for the purposes of the administration of this Act." *Id.* § 6(6). Also, "[a]ccess to the information in the crime scene index shall be permanently removed, in accordance with any regulations that may be made under this Act, if the information relates to a DNA profile derived from a bodily substance . . ." *Id.* § 8.1. Furthermore,

> Access to the following information in the convicted offenders index shall be permanently removed without delay after
>
> (a) in the case of information in relation to a person who has been convicted of a designated offence, the conviction is quashed and a final acquittal entered; and
>
> (b) in the case of information in relation to a person who has been discharged under section 730 of the Criminal Code of a designated offence,
>
> (i) the expiry of one year after the person is discharged absolutely, unless the person is convicted during that year of another offense, or
>
> (ii) the expiry of three years after the person is discharged conditionally, unless the person is convicted during those three years of another offence.

Id. § 9(2)(a), (b)(i)–(ii). *See also* W. AUSTL. POLICE SERV., SAMPLE DESTRUCTION, http://www.police.wa.gov.au/AboutUs/AboutUs.asp?DestructionDNA (last visited Jan. 23, 2005). In relevant part, the Australian website provides:

> If you are a suspect for an offence then you may request your identifying particulars to be destroyed if after two years you have not been charged with a relevant offence or you are found not guilty of the offence you have been charged with.

may request that either the sample be destroyed after a not-guilty verdict or within a period of two years provided no charge is brought.[87] The *Kincade* plurality left for another day whether individuals like Mr. Kincade might be entitled to have their DNA removed from CODIS once their status changes.[88]

C. The potential exists for national and international government entities to obtain unregulated access to profiles housed in CODIS

It is possible that DNA databases may soon be linked for the purpose of sharing genetic material on a global scale. The National Criminal Information Center (NCIC) contains criminal history records of more than fifty-two million individuals.[89] This system does not currently interface with CODIS, but that may soon change.[90] However, NCIC does interface with U.S. Visitor & Immigration Status Technology (US-VISIT), which was recently implemented at 115 airports and 15 seaports and makes the determination as to which visitors may or may not enter the country.[91] The Terrorist Identification Database Act of 2003, embedded within the Domestic Security Act of 2003 and colloquially referred to as "Patriot Act II,"[92] would empower the Attorney General to collect DNA samples for the purpose of "detecting, investigating, prosecuting, preventing or responding to terrorist activities."[93] The possibility of a national identity system could amplify these potential privacy invasions.[94]

> If you have been charged with a serious offence, you may request your identifying particulars to be destroyed if you are found not guilty of the offence you have been charged with.

Id.

87. *Id.* In fact, several countries, including New Zealand, Germany, Sweden, Denmark and the Netherlands have implemented rules that require destruction of the sample after the creation of a profile. AUSTL. LAW REFORM COMM'N, ALRC 96 ESSENTIALLY YOURS: THE PROTECTION OF HUMAN GENETIC INFORMATION IN AUSTRALIA 1034, http://www.austlii.edu.au/au/other/alrc/publications/reports/96/41_Criminal_Investigations.doc.rtf (last visited Oct. 27, 2005).

88. United States v. Kincade, 379 F.3d 813, 874 (9th Cir. 2004) (Kozinski, J., dissenting).

89. FBI, U.S. DEP'T OF JUSTICE, PROTECTING AMERICAN STREETS: LAW ENFORCEMENT INFORMATION SHARING IS KEY! (Jan. 7, 2004), http://www.fbi.gov/page2/jan04/cjis010704.htm.

90. The possibility of using these systems to interface with one another has been proposed. *See, e.g.*, BUREAU OF IMMIGRATION & CUSTOMS ENFORCEMENT, U.S. DEP'T OF HOMELAND SEC., ENDGAME: OFFICE OF DETENTION & REMOVAL STRATEGIC PLAN, 2003-2012 4-8 (Aug. 15, 2003), *available at* http://www.ice.gov/graphics/dro/endgame.pdf.

91. DEP'T OF HOMELAND SEC., US-VISIT PROGRAM, INCREMENT 1, PRIVACY IMPACT ASSESSMENT (Dec. 18, 2003), *available at* http://www.epic.org/privacy/us-visit/us-visit_pia.pdf.

92. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

93. *See* Scheeres, *supra* note 28. "The proposed database grants law enforcement agencies unprecedented access to private genetic information, allowing investigators to seize DNA samples from people merely *suspected* of participating in a broad number of activities that qualify as domestic

Furthermore, these privacy invasions could be exacerbated by mass expansion of databanking, a prospect that many lawmakers, scientists, and scholars fiercely advocate. The United Kingdom has already considered the possibility of a "universal" database.[95] Alec Jeffreys, the author of the DNA technology to identify suspects, has endorsed this prospect.[96] In 1998, New York Mayor Rudolph Guiliani offered support for a universal database, asking the legislature to consider mandatory DNA extraction of all newborns as a crime prevention measure.[97] Many other academic

---

terrorism, a new crime that was ushered in by the original Patriot Act." *Id.* Civil libertarians suggest that such legislation would allow police to take DNA samples from war protestors under the auspices of the war on terrorism. *Id.* In addition, former Attorney General John Ashcroft endorsed legislation proposed by the FBI to establish a DNA database for suspected terrorists. David Johnston, *Law Change Sought to Set up DNA Databank for Captured Qaeda Fighters*, N.Y. TIMES, Mar. 6, 2002, at A13. Furthermore, President Bush has more recently advocated setting up a DNA database of people associated with terrorist groups. Dana Milbank, *President Asks for Expanded Patriot Act: Authority Sought to Fight Terror*, WASH. POST, Sept. 11, 2003, at A1. See also Chang, *Trampling on the Bill of Rights*, *supra* note 10; Marjorie Cohn, *America: A Nation of Snitches?*, SAN DIEGO UNION-TRIB., July 18, 2002, at B7.

94. *See* Daniel J. Steinbock, *National Identity Cards: Fourth and Fifth Amendment Issues*, 56 FLA. L. REV. 697 (2004) (discussing the merits and constitutional restraints on a national identity card as a tool against terrorists and a response to illegal immigration, identity theft, and electoral fraud). Steinbock's forecast could easily include DNA databases to store individual data for purposes of the national identity card.

> Any such system depends on two major features: the database (or databases) containing information about particular individuals and the means to connect a given person with that information. One way to store information about a person is on a card or other physical token in human-readable or machine-readable form. Alternatively, information may be stored in computer databases elsewhere, in which case there will likely be points in time at which information about the individual would be accessed or input or both. . . . What data to collect, who would have access to that data, and what uses would be made of it are major issues in the design of any prospective national identity system.

Id. at 703.

95. The United Kingdom has already launched a "Biobank" effort, a voluntary national DNA database of a half million citizens, designed to study the interaction of genes, environment and health. Rosen, *supra* note 5, at 43. Ultimately, pharmaceutical and biotechnology companies will be given access to the database "to develop new drugs and treatments." *Id.* at 44.

96. *Id.* "If the correct safeguards are in place to protect civil liberties, why should a proposal to test everyone at birth be a frightening one?" *Id.* at 45 (quoting two Australian researchers). This proposal is supported as well by James Watson, co-discoverer of the structure of DNA. *Id.* Watson noted that "It's hard to imagine that in 100 years from now we won't have [a universal DNA database]. With the increase in terrorism, we want to know who people are." *See* Nicholas Pyke, *"Genetic Bank" Call by Father of DNA*, THE GUARDIAN, Feb. 3, 2003. For a scholarly proposal for universal DNA databases, see John P. Cronan, *The Next Frontier of Law Enforcement: A Proposal for Complete DNA Databanks*, 28 AM. J. CRIM. L. 119, 122 (2000) (discussing the "unprecedented law enforcement benefits" from a system for storing DNA samples at birth); *but see* Rebecca Sasser Peterson, Note, *DNA Databases: When Fear Goes too Far*, 37 AM. CRIM. L. REV. 1219 (2000) (arguing that allowing searches and seizures of DNA of every citizen absent a warrant would be unconstitutional).

97. See David Seifman, *Getting DNA Samples at Birth Fine with Rudy*, N.Y. POST, Dec. 17, 1998, at 34.

sources and law enforcement agencies have argued for a complete national database.[98]

The U.S. Senate has arguably started moving in this direction through a recent amendment to the Violence Against Women Act of 2005 (VAWA).[99] Introduced by Senator Kyl in July of 2005[100] and passed by the Senate in October of 2005,[101] the DNA Fingerprint Act of 2005 will "[e]liminate federal statutory restrictions that prevent an arrestee's DNA sample from being included in NDIS as soon as he is charged in a pleading,"[102] removing barriers to profiling increasing amounts of data from criminal arrestees. The Council for Responsible Genetics has written to the Senate Judiciary Committee and urged that this amendment be dropped from the Act, as it "undermines the principle of presumptive innocence and renders [an arrestee] an automatic suspect for any future crime. While it has been argued . . . that convicted felons forfeit this basic right of privacy . . ., this cannot be said for people who are merely arrested or detained, many of whom are innocent."[103]

---

98. *See, e.g.*, Peterson, *supra* note 96, at 1228 ("A universal DNA database containing a DNA fingerprint from every citizen of the United States could be used to identify otherwise missed first-time offenders and to render unnecessary discriminatory dragnets."); Michelle Hibbert, *DNA Databanks: Law Enforcement's Greatest Surveillance Tool?*, 34 WAKE FOREST L. REV. 767, 817 (1999):

> [i]f courts are to continue to view the collection of DNA samples—either through cheek scrapings, strands of hair . . . or drawing blood samples—as a slight intrusion, and legislatures are to continue to highly value DNA databanks for their crime solving potential, then it may not seem unreasonable to require the DNA databanking of all persons.

Id. Yale University professor Akhil Amar contemplates a universal DNA database with a biological sample from as many citizens as possible:

> Every newborn now has a medical blood test; a few drops could be sent to a DNA lab. Adults could undergo a cheek swab when they renew their drivers' licenses, for example. . . . This data would be stored in computers and could be checked against any genetic material found at crime scenes.

Akhil Reed Amar, *A Search for Justice in Our Genes*, N.Y. TIMES, May 7, 2002, at A31.

99. Violence Against Women Act of 2005, S. 1197, 109th Cong. (2005) (reauthorizing the Violence Against Women Act of 1994).

100. *See* Office of Senator John Kyl, Press Release, *Senate ReAuthorizes Violence Against Women Act*, Oct. 5, 2005, http://kyl.senate.gov (follow "Press Releases" hyperlink under "Media Resources") [hereinafter Kyl Press Release].

101. Violence Against Women Act of 2005, S. 1197, 109th Cong., tit. X, §§ 1001–05 (as passed by Senate, Oct. 4, 2005).

102. Kyl Press Release, *supra* note 100.

103. Letter from Sujatha Byravan, Ph.D., President, Council for Responsible Genetics, to Senate Judiciary Committee on the DNA Fingerprint Act of 2005 (Nov. 5, 2005), *available at* http://www.gene-watch.org/press/DNADatabase11-7-05.html.

IV. STORAGE OF PRIVATE INFORMATION: *WHALEN V. ROE*

The 1977 Supreme Court opinion in *Whalen v. Roe*[104] bears perhaps as much resemblance to *Kincade* as does the line of Fourth Amendment "search" cases.[105] The holding embraced a law enforcement interest in tracking personal medical information of individuals who had not committed, nor were suspected of committing, any crime.[106] The analysis centered on invasion of privacy concerns rather than the Fourth Amendment and recognized for the first time the concept of a right to informational privacy.[107] The prevailing concerns of the *Whalen* plaintiffs were similar to those of individuals like Mr. Kincade—namely,

---

104. 429 U.S. 589 (1977).

105. For links between privacy of informational content and Fourth Amendment searches, see James J. Tomkovicz, *Technology and the Threshold of the Fourth Amendment: A Tale of Two Futures*, 72 MISS. L.J. 317 (2002). "If informational privacy is the core interest safeguarded by constitutional control over searches . . . then it seems eminently sensible to link the scope of Fourth Amendment governance to the potential for disclosures of matters with 'informational content.'" *Id.* at 382.

In current form, "there are no legal safeguards that prevent the possible misuse of information contained in CODIS by foreign law enforcement agencies" and no underlying federal protection has been put in place to "forbid the use of samples [from the databases] for other purposes." EPIC Brief, *supra* note 71, at 15.

106. *See Whalen*, 429 U.S. at 873 (New York State Controlled Substance Act of 1972 required prescriptions for Schedule II drugs to be prepared in triplicate and sent to New York State Department of Health).

107. The *Whalen* Court recognized that an individual's "interest in avoiding disclosure of personal matters" is an aspect of the right of privacy. 429 U.S. 589, 598–600 & nn.23–25 (1977). The holding was the first to specifically recognize an individual's right to information privacy, as distinct from the "interest in independence in making certain kinds of importance decisions." 429 U.S. at 599–600. *See* Jean Slemmons Stratford & Juri Stratford, *Data Protection and Privacy in the United States and Europe*, IASSIST QUARTERLY 17 (Fall 1998), *available at* http://iassistdata.org/publications/iq/iq22/iqvol223stratford.pdf. The original privacy jurisprudence derived from Samuel Warren and Louis Brandeis, who in 1890 defined the right to privacy as "the right to be let alone." Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890). Subsequently, *Katz v. United States* addressed the issue of individual privacy, holding that electronic eavesdropping was a "search" because it had "violated the privacy upon which [Katz had] justifiably relied." Katz v. United States, 389 U.S. 347, 353 (1967). Justice Harlan stated famously in a concurring opinion that "[t]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Id.* at 361 (Harlan, J., concurring).

Building on opinions from *Katz*, *Griswold v. Connecticut*, 381 U.S. 479 (1965) (state law prohibiting the use of contraceptives is unconstitutional and intrudes on "zones of privacy" created by the Bill of Rights) and *Roe v. Wade*, 410 U.S. 113, 153 (1973) (personal liberty allows a woman the "decision whether or not to terminate her pregnancy"), the *Whalen* Court acknowledged that the "'right of privacy' is founded in the Fourteenth Amendment's concept of personal liberty." *Whalen*, 429 U.S. at 599 n.23. "Under *Katz*, the crucial threshold question for DNA sampling is whether society should recognize as reasonable the expectation that the sample is not 'up for grabs' by the government." D.H. Kaye, *The Constitutionality of DNA Sampling on Arrest*, 10 CORNELL J.L. & PUB. POL'Y 455, 473 (2001).

possibilities of discrimination based on discovery of the stored information.[108]

In *Whalen*, physicians and patients in New York challenged the constitutionality of the New York State Controlled Substances Act of 1972,[109] requiring doctors to provide the state with copies of prescriptions for certain classes of drugs.[110] Under the law, the state maintained records of names and addresses of all such individuals in a centralized computer file.[111] The purported goal was to track the possession and consumption of drugs for which there was a legitimate as well as illegitimate market, in effort to prevent the use of stolen or revised prescriptions.[112] The physicians and patients raised fears that potential misuse of the data stored by the state might cause them to be labeled unfairly as "drug addicts."[113] The state vehemently argued the reasonableness of the storage by declaring that "the patient-identification requirement might aid in the enforcement of laws designed to minimize the misuse of dangerous drugs."[114] The Court held that the New York program did not pose a threat "sufficiently grievous" to amount to a constitutional violation,[115] reasoning that

> [t]here is no support in the record . . . that the security provisions of the statute will be administered improperly. And the remote possibility that judicial supervision of the evidentiary use of particular items of stored information will provide inadequate protection against unwarranted disclosures is surely not a sufficient reason for invalidating the entire patient-identification program.[116]

---

108. *See infra* note 113 and accompanying text.

109. N.Y. PUB. HEALTH LAW § 3300–97 (McKinney 2002).

110. *Whalen*, 429 U.S. 589.

111. *Id.* at 592.

112. *Id.* The New York statute distinguished between different classes of drugs. "Drugs, such as heroin . . . are in Schedule I . . . Schedules II through V include drugs which have a progressively lower potential for abuse but also have a recognized medical use." *Id.* The State was concerned mostly with drugs that fell into the Schedule II category. *Id.* To provide a picture of drug volume involved at the time under this law, the District Court determined that "about 100,000 Schedule II prescription forms are delivered to a receiving room at the Department of Health in Albany each month. They are sorted, coded, and logged and then taken to another room where the data on the forms is recorded on magnetic tapes for processing by a computer." *Id.* at 593.

113. *Id.* at 595. Among concerns raised was also the prospect that patients were declining the medical treatment because of their fears of stigmatization. *Id.*

114. *Id.* at 597–98. The State also argued the utility in aiding detection of potential instances of abuse. *Id.*

115. *Id.* at 600.

116. *Id.* at 601–02.

While recognizing a "remote possibility" of abuses of the computerized storage system, the Court summarily dismissed the concerns over stigmatization and potential discrimination should the information somehow leak.[117] Of note is the fact that in 1977, the concept of computerized storage in mainframes was nascent in development, and public knowledge of the potential to hack into a system and gain access to its contents was not common.[118] A few decades later, this very possibility is no longer remote. Now with information so readily accessible through means of new technology, pharmaceuticals and health care providers have, on numerous documented occasions, chosen to exploit the very information that the plaintiffs in *Whalen* were concerned with guarding.[119]

---

117. *Id.* at 601. The *Kincade* plurality responded to Judge Reinhardt's parade of horribles scenario in a manner not dissimilar to the *Whalen* Court. United States v. Kincade, 379 F.3d 813, 837 (9th Cir. 2004). Though noting that Judge Reinhardt's concerns were "weighty ones, and we do not dismiss them lightly," the court did not accord them great reflection, reasoning that "our job is limited to resolving the constitutionality of the program before us, as it is designed and as it has been implemented." *Id.* at 837–838. Further,

> In our system of government, courts base decisions not on dramatic Hollywood fantasies, but on concretely particularized facts developed in the cauldron of the adversary process and reduced to an assessable record. If . . . and when, some future program permits the parade of horribles the DNA Act opponents fear . . . we have every confidence that courts will respond appropriately.

Id. (citations omitted).

118. In spite of this, Justice Brennan wrote a concurring opinion in *Whalen* expressing similar concerns as did Judge Reinhardt three decades later:

> What is more troubling about this scheme, however, is the central computer storage of the data thus collected. Obviously, as the State argues, collection and storage of data by the State that is in itself legitimate is not rendered unconstitutional simply because new technology makes the State's operations more efficient. However, as the example of the Fourth Amendment shows the Constitution puts limits not only on the type of information the State may gather, but also on the means it may use to gather it. The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology.

Whalen, 429 U.S. at 606–07 (Brennan, J. concurring).

119. In 2002, for example, a Florida woman who was in treatment for depression filed suit against Eli Lilly & Co., her doctors and her pharmacy, Walgreens, when she received a month's free trial sample of the drug Prozac Weekly in the mail. *See* Betsy Spethmann, *Prozac Nightmare*, PROMO MAGAZINE, Sept. 1, 2002, *available at* http://promomagazine.com/mag/marketing_prozac_nighmare/index.html. The sample was enclosed with a letter, which cheerily stated, "'Dear Patients, we are very excited to be able to offer you a more convenient way to take your antidepressant medication. For your convenience, enclosed you will find a FREE one-month trial of Prozac Weekly.'" *Unsolicited Prozac Weekly Mailed to Patients*, PSYCHOPHARMACOLOGY UPDATE, Aug. 1, 2002, *available at* 2002 WLNR 10809080. While Lilly responded to the lawsuit by disciplining sales managers and representatives, it plainly appears the samples were part of a very active attempt to solicit customers to return to a Lilly drug. Glenn Singer, *Eli Lilly Suspends Several Employees Over Mailing of Free Prozac Samples*, SOUTH FLORIDA SUN-SENTINEL, Jul. 9, 2002, *available at* 2002 WLNR 10617265. Where, exactly, the breakdown occurred is unclear, and, not surprisingly, hotly disputed by Lilly and Walgreens. Most likely, Walgreens was involved in covertly marketing patient lists to Lilly. The pharmacy very likely

And in fact, legislation from the decade surrounding the *Whalen* decision indicates that President Gerald Ford and Congress were fully cognizant of the need to safeguard individual privacy in personal information.[120] The Court did note that it was "not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[121] The Court also recognized that "[t]he right to collect and use such data for public purposes

---

"allowed access to patient prescription records, providing Lilly with a list of antidepressant users." Lauran Neergaard, *Lawsuit After Prozac Arrives in Mail*, AP ONLINE, Jul. 6, 2002, *available at* 2002 WL 23894011.

The concerns about privacy of medical records are not restricted to unsolicited Prozac. Numerous leaks of pharmacy records, without patients' consent, have led to discrimination of a magnitude not imagined by the 1977 Court. For example, as with genetic discrimination, the potential is great for private information to reach employers, who may use it to deny promotions or avoid hiring in the first place. In 1998, Ben Walker, a 30-year FBI veteran received a demotion, was forced to hand in his gun, was taken off drug cases and put on administrative leave because the Bureau had obtained pharmacy records which indicated Walker was using anti-depressants. Alissa J. Rubin, *Records no Longer for Doctors' Eyes Only; In Today's Health Care System, Outside Parties Such as Insurers and Employers have Access to Patients' Once-Private Medical Information, Resulting Horror Stories Have Some Seeking New Rules*, L.A. TIMES, Sept. 1, 1998, at A1. According to the article, "[i]n a 1996 survey of Fortune 500 companies by researchers at the University of Illinois, 35% said they had used individual medical information to make job-related decisions." *Id.* The number has most likely increased in the past decade. "What makes the issue so difficult is that—although patients want privacy—employers, insurers and public health agencies have an interest in controlling costs, rooting out fraud, tracking infectious diseases and finding the most effective treatments for different ailments." *Id.* The news article also outlines several "questionable cases," such as two east coast pharmacy chains, CVS and Giant, which shared confidential prescription information with drug manufacturers for target marketing and customer tracking. *Id.* The paper record of a single medical encounter is significant. For a checkup or visit to a specialist, "[o]n average, the paper record . . . makes 17 stops in the health care system, from the physician, lab staff and pharmacy personnel, to health and life insurance managers, researchers, state vital statistics bureaus and more, according to an analysis presented a meeting on health privacy" in 2001 in Washington. M.A.J. McKenna, *With Online Boom, Privacy Worries Loom Ever Larger*, THE ATLANTA JOURNAL-CONSTITUTION, Apr. 22, 2001, at 1F.

This scenario is alarming to physicians as well as patients. According to Dr. Nancy Dickey, a Texas physician who was head of the American Medical Association's board of trustees, "Our worst-case scenario is that patient-specific data becomes centrally available and patients become unable to get insurance, unable to get jobs and unwilling to share information with me because of fear of where it will end up." John Riley, *When you Can't Keep a Secret; Insurers' Cost-Cutters Demand Your Medical Details*, NEWSDAY (New York), Apr. 1, 1996, at A7.

120. *See* Privacy Act of 1974, Pub. L. No. 93–579, 88 Stat. 1896 (codified at 5 U.S.C. § 552a (1988)) [hereinafter "Privacy Act"]. With an onset of technological advances in the 1970s, public and congressional apprehension over invasions of individual privacy spurred the enactment of the Privacy Act. For further elaboration on the congressional findings accompanying the Act, see *Privacy: The Collection, Use and Computerization of Personal Data: Joint Hearings Before the Subcomm. on Privacy and Information Systems of the S. Comm. on the Judiciary*, 93d Cong., 2d Sess. (1974) (discussion of potential threat to informational privacy that computerized informational systems maintained by the federal government pose to the public); *Federal Databanks, Computers and the Bill of Rights: Hearings Before the Subcomm. on Constitutional Rights of the S. Comm. on the Judiciary*, 92d Cong., 1st Sess. (1971) (similar).

121. *Whalen*, 429 U.S. at 605.

is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures."[122] In stating this, however, the Court declined to consider questions that might be presented by the potential unwarranted disclosure, whether intentional or unintentional, of the private data.[123]

V. ANALYSIS

Though Judge Reinhardt maintained in his *Kincade* dissent that the Supreme Court had "never once" in history approved a suspicionless search "designed to produce ordinary evidence of criminal wrongdoing for use by the police,"[124] the Court has approved large-scale databanking of private information for that purpose.[125] And indeed, *Whalen's* validation of a law enforcement interest in favor of storing private information, when taken together with *Kincade's* totality of the circumstances approval of DNA testing post-conviction felons, gives "reason to fear that the nightmarish worlds depicted in films such as *Minority Report* and *Gattaca* will become realities."[126] With the continued expansion of law enforcement interests, as well as the expansion of crimes recordable in CODIS, the trend is plainly moving toward establishing a law enforcement interest in tracking increasingly larger groups of the populous, even in the absence of specific individualized suspicion.[127] The trend's rationale continues to hinge on Fourth Amendment analysis.[128] Given the context of the United States' entrenchment in fighting the "war on terror,"[129] there is even more reason to be wary of expanding governmental and law enforcement powers without the rigor of fine constitutional analysis.[130]

---

122. *Id.*

123. *Id.* at 605–606.

124. United States v. Kincade, 379 F.3d 813, 854 (9th Cir. 2004) (Reinhardt, J., dissenting).

125. *See supra* notes 114–17 and accompanying text.

126. *Kincade*, 379 F.3d at 851 (Reinhardt, J., dissenting).

127. *See* Solove, *Digital Dossiers*, *supra* note 53, at 1084 ("In the aftermath of the terrorist attacks of September 11, 2001, the impetus for the government to gather personal information has greatly increased, because such data can be useful to track down terrorists and to profile airline passengers for more thorough searches.").

128. *See* Solove, *Digital Dossiers*, *supra* note 53, at 1096 ("Law enforcement officials have a greater desire to obtain information that could be helpful in identifying terrorists or their supporters, including information about what people read, with whom they associate, their religion, and their lifestyle."); *see also supra* note 26 and accompanying text.

129. *See* Richard W. Stevenson, *President Makes it Clear: Phrase is 'War on Terror*,' N.Y. TIMES, Aug. 4, 2005, at A12.

130. *See supra* note 19 and accompanying text. Indeed, former U.S. Supreme Court Justice Sandra Day O'Connor remarked, upon visiting Ground Zero in the wake of September 11th, "[w]e're likely to experience more restrictions on personal freedom than has ever been the case in this country." Linda

The Supreme Court's line-drawing in the battery of Fourth Amendment cases involving forced blood or urine testing focuses on a reasonableness inquiry with two main threads. First, there must be a special need transcending normal law enforcement interests, such as mandatory drug testing of student athletes, mandatory drug and alcohol testing of railway employees, or mandatory sobriety testing at highway checkpoints.[131] Second, the intrusion on the individual's privacy must be minimal.[132] Cases that have examined forced extraction of DNA samples, including *Kincade*, have emphasized the diminished expectation of privacy that convicted felons experience.[133] Supreme Court cases have also noted that student athletes experience a similar diminished expectation of privacy once they choose to be part of a team, as noted in Reinhardt's dissent.[134]

Using the Supreme Court's balancing test,[135] there is certainly room to argue that there is a "special need" in maintaining DNA databases of individuals who may be more likely, based on previous behavior or predisposition, than others to commit crimes.[136] A "special needs"

Greenhouse, *In New York Visit, O'Connor Foresees Limits on Freedom*, N.Y. TIMES, Sept. 29, 2001, at B5.

131. *See supra* note 58–64 and accompanying text. *See also* Mark A. Rothstein & Sandra Carnahan, *Legal and Policy Issues in Expanding the Scope of Law Enforcement DNA Data Banks*, 67 BROOK. L. REV. 127, 138–44 (2001) (discussing the Supreme Court balancing test as applied to special needs cases). "Courts must balance the degree of intrusion upon an individual's privacy against the government interest at stake." *Id.* at 138.

132. *Id.*

133. *See supra* notes 39–44 and accompanying text. As articulated in *Kincade*, "the Court has recognized that 'those who have suffered a lawful conviction' are properly subject to a 'broad range of [restrictions] that might infringe constitutional rights in free society' . . . in no small part due to the extraordinary rate of recidivism among offenders." United States v. Kincade, 379 F.3d 813, 833 (9th Cir. 2004) (citation omitted). Further,

> We believe that such a severe and fundamental disruption in the relationship between the offender and society, along with the government's concomitantly greater interest in closely monitoring and supervising conditional releasees, is in turn sufficient to sustain suspicionless searches of his person and property even in the absence of some non-law enforcement "special need"—at least where such searches meet the Fourth Amendment touchstone of reasonableness as gauged by the totality of the circumstances.

Id. at 835.

134. *See* Bd. of Educ. of Indep. Sch. Dist. No. 92 v. Earls, 536 U.S. 822 (2002); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995).

135. Of note, the Ninth Circuit's decision did not center on a parolee's diminished expectation of privacy, but rather, the fact that the minimal intrusion was outweighed by the great potential crime-fighting capability. *See Kincade*, 379 F.3d at 833–35.

136. There are multiple arguments for expanding the scope of DNA databases at the national level: "to aid medical research, to create the biotechnology economy of the future, or to ensure that every falsely accused citizen has a genetic alibi." Rosen, *supra* note 5, at 43. Other arguments suggest that potential links between genetics and behavior might help to predict whether certain individuals might be naturally more violent than others. For a discussion on the implications of genetics and crime, see Elkins, *supra* note 9, at 296–305 ("'Scientists have in fact isolated certain genes that

justification for law enforcement storage of DNA for potential future "cold hits" arguably resembles the rationale used in similar cases addressing a government interest in highway sobriety tests, drug and alcohol testing of railroad employees, and roadside checkpoints to catch illegal aliens.[137] The "special needs" justification might be articulated as increased conviction rates, deterrence leading to a lower rate of crime, reduction of wrongful arrests, propelling the war against terror, and the privacy intrusion may become de minimis.[138] Given that the Court has endorsed "special needs" exceptions in cases where individuals experience a reduced expectation of privacy,[139] we may soon reach the point where the "war on terror" demands reduced expectations of privacy for all citizens.[140]

The Ninth Circuit virtually eschewed the "special needs" analysis and chose to employ the more murky "totality of the circumstances" test, which provides even less of a restraint on future Fourth Amendment

---

indicate an increased susceptibility to certain diseases;' as well as evidence that 'a person's IQ, emotional temperament, and certain other mental qualities have causal antecedents in his genetic structure.'") (quoting Hugh Miller, III, *DNA Blueprints, Personhood, and Genetic Privacy*, 8 HEALTH MATRIX 179, 204 (1998)).

137. *See supra* notes 39–44 and accompanying text.

138. *See generally* Cronan, *supra* note 96, at 148–51; *see also* Rothstein & Carnahan, *supra* note 131, at 142 ("With new technology, the physical intrusions required in collecting DNA may be de minimis. If the courts balance this minimal physical intrusion against the government interest, then even broader DNA testing for law enforcement might be upheld.")

139. *See, e.g.*, *Acton*, 515 U.S. at 656–57 (reduced expectation of privacy among student athletes choosing to compete on a team); Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 672 (1989) (individuals working as customs agents have reduced privacy expectations); Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 624–625 (1989) (railway workers in a highly regulated industry have a reduced expectation of privacy).

140. The United States may have already reached this point. In The 9/11 Commission Report of August 2004, formally titled "The Final Report of the National Commission of Terrorist Attacks Upon the United States," the recommendations of the House Judiciary Committee included the federalization of drivers' licenses, currently a state responsibility. *See 9/11 Commission Report: Civil Liberties Implications*, WASHINGTON NEWSLETTER (No. 691) (Friends Committee on National Legislation), Oct. 2004, at 3, 7 *available at* http://www.fcnl.org/now/pdf/oct04.pdf. "This proposal would necessitate a new national bureaucracy and database structure built around individual identifiers, such as names or identification numbers (like social security numbers), or some biometric indentifiers (fingerprints, iris scans, and facial scans that can be embedded in a computer chip in a national card)." *Id.* at 3. Such a system could be linked to or built upon genetic identifiers such as individual DNA. Some scholars point out that because we tolerate minimal Fourth Amendment intrusions in the interest of increased security, such as metal detectors at airports, using DNA to solve crimes and prevent forms of identity fraud "could actually make Americans more 'secure in their persons, houses, papers, and effects.'" Akhil Reed Amar & Vikram David Amar, *A Dialogue on why Mandatory DNA Tests are Different From Mandatory Drug Tests for Fourth Amendment Purposes*, May 17, 2002, http://writ.findlaw.com/amar/20020517.html. "[M]etal detectors at airports [are] quintessential examples of reasonable searches and seizures, even though these airport encounters lack individualized suspicion. Such metal detectors are nondiscriminatory, relatively unintrusive, well justified, and broadly accepted by the public." *Id.*

contests.[141] The use of such a vague balancing test sets a bold precedent. The *Whalen* Court's use of a similar balancing test, which allowed for storage of highly personal information,[142] adds credence to *Kincade's* holding. Together, these cases indicate that computerized storage of personal private records is permissible with no individualized suspicion, even employing a lesser burden than the "special needs" inquiry. By analogy, so should be samples of DNA. Even so, the loyalty to a strict Fourth Amendment analysis under either the "special needs" or "totality of the circumstances" rubric seems to disregard crucial distinctions between searches and permanent storage of unique genetic identifiers.

While outer limits of privacy are not enumerated in the text of the Constitution,[143] it is clear among Supreme Court decisions that an individual may make, without unjustified government intrusion, personal decisions relating to marriage,[144] procreation,[145] contraception,[146] a woman's destiny and body,[147] family relationships,[148] and child rearing and education.[149] In *Griswold v. Connecticut*, Justice Douglas' plurality opinion toyed with the notion that various rights are provided under "penumbras" of the Constitution.[150] Some scholars have attempted, with

---

141. Judge Reinhardt expressed wariness at granting the government more authority to fight crime, especially when a symptom of this authority is dismantling core values of the Fourth Amendment:

> My colleagues would abandon the restraints that the special needs doctrine places on the government's ability to conduct blanket searches. In that doctrine's place, they would leave us with nothing more than a boundless test that will inevitably side with the "monumental" law enforcement interests at stake and with the empty promise that the state will exercise restraint if the circumstances so demand.

United States v. Kincade, 379 F.3d 813, 870 (9th Cir. 2004) (Reinhardt, J., dissenting).

142. *See supra* note 116 and accompanying text.

143. In *Griswold v. Connecticut*, 381 U.S. 479, 484 (1965), the Court recognized that "[v]arious guarantees create zones of privacy." According to Professor Daniel Solove, "Privacy law consists of a mosaic of various types of law: tort law, constitutional law, federal and state statutory law, evidentiary privileges, property law, and contract law. Privacy law is best described with the notion of the *bricoleur*—a person who uses whatever is at hand as a tool to solve problems." Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1430 (2001) [hereinafter Solove, *Privacy and Power*].

144. Loving v. Virgina, 388 U.S. 1, 12 (1967).

145. Skinner v. Oklahoma, 316 U.S. 535, 541–42 (1942).

146. Eisenstadt v. Baird, 405 U.S. 438, 453–54 (1972).

147. Roe v. Wade, 410 U.S. 113 (1973).

148. Prince v. Massachusetts, 321 U.S. 158, 166 (1944).

149. Pierce v. Soc'y of the Sisters of the Holy Names of Jesus & Mary, 268 U.S. 510, 535 (1925).

150. Griswold v. Connecticut, 381 U.S. 479, 484 (1965). The *Griswold* opinion conceived of a right to privacy primarily in terms of physical and in some ways decisional privacy, but did not expressly consider informational privacy:

> [S]pecific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy.

limited success, to extract informational privacy protections out of *Griswold*, *Eisenstadt v. Baird*, and *Roe v. Wade*.[151] The judicial territory relating to informational privacy interests being cloudy,[152] perhaps it is time for a re-examination of the legal implications of not only extracting a blood sample, but storing private genetic information indefinitely. If the focus of the analysis were shifted from the mere collection of information to the actual substance of information taken and stored, it becomes evident that any storage and use of personal information is an invasion of that person's privacy.[153] The fact that the information can be accessed numerous times over long, and perhaps indefinite, periods of time makes the practice of storing personal DNA distinct from traditional Fourth Amendment searches.[154] While the Court has not offered much elaboration

---

> The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."

Id. (citation omitted).

151. *See, e.g.*, Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815 (2000). Privacy rights may arguably be "implicit in the concept of ordered liberty," and thus encapsulated by the due process clause of the Fourteenth Amendment, according to Justice Cardozo. Palko v. Connecticut, 302 U.S. 319 (1937).

152. "American privacy law is . . . vast and complex, extending beyond torts to the constitutional 'right to privacy,' Fourth Amendment law, evidentiary privileges, dozens of federal privacy statutes, and hundreds of state privacy statutes." Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006). Because there is no specifically delineated constitutional "right to privacy" to point to, the analysis of storing DNA samples in a database has been construed under a recognizable constitutional right and judicial doctrine: protection from unreasonable searches under the Fourth Amendment. *See, e.g.*, United States v. Kincade, 379 F.3d 813 (9th Cir. 2004); Green v. Berge, 354 F.3d 675 (7th Cir. 2004); Jones v. Murray, 962 F.2d 302 (4th Cir. 1992).

153. *See* Viktor Mayer-Schönberger, *Strands of Privacy: DNA Databases and Informational Privacy and the OECD Guidelines*, *in* DNA AND THE CRIMINAL JUSTICE SYSTEM: THE TECHNOLOGY OF JUSTICE (David Lazer ed., The MIT Press 2004). "Indeed, DNA databases pose a privacy threat not because of the way samples are taken but because of the information inherent in the samples." *Id.* at 226. Mayer-Schönberger, in this Kennedy School of Government research paper, adds an explanation for the judicial and scholarly focus on DNA extraction as a Fourth Amendment concern:

> [T]he potential danger is the information distilled from the DNA sequences and even more precisely the use of such information being outside of the control of the individual. But because control over information is connected with informational privacy, a value not explicitly protected by present constitutional privacy jurisprudence, commentators have refocused their scrutiny towards the activity afforded some Constitutional protection, the collection of the DNA samples.

Id.

154. *See* Mayer-Schönberger, *supra* note 153, stating that "[t]he privacy intrusion happens *every time* an individual's record is accessed as part of a search. Every time this happens the balancing has to

post-*Whalen* on decisional or informational privacy rights,[155] a "right to privacy" has been recognized in many circuits.[156] In addition, extraction and storage of DNA may implicate substantive due process rights, such as the right to make decisions concerning one's own body.[157] This element, in combination with the Fourth Amendment and informational privacy, further suggests that stricter scrutiny should be considered for purposes of evaluating the constitutionality of DNA extraction.[158] Perhaps an era is approaching in which further examination of privacy rights by the Court would help to inform analysis of DNA extraction and perhaps mitigate the potential civil liberties ramifications addressed above.[159]

State and federal laws have rapidly increased the list of qualifying crimes for entry into a DNA database.[160] The fact that some states allow for DNA extraction upon arrest, before an individual has even been tried, is evidence of this trend.[161] Even beyond the prospect of DNA testing

---

take place and the benefits have to outweigh the intrusion." *See also* Solove, *supra* note 152, stating in an effort to suggest a new "taxonomy" for privacy rules that, among stages of 1) information collection, 2) information processing, 3) information dissemination and 4) invasion, "[t]he collection of [personal] information itself can constitute a harmful activity."

155. Shortly after *Whalen*, the Court read an informational privacy right into President Nixon's private communications with his family, as opposed to records involving his official duties in *Nixon v. Administrator of General Services*, 433 U.S. 425 (1977). *See* Solove, *Privacy and Power*, *supra* note 143, at 1438. However, the Court has done little else to develop the doctrine. *Id.*

156. *See, e.g.*, Doe v. Borough of Barrington, 729 F. Supp. 376 (D.N.J. 1990) (police disclosing to neighbors that member of community had AIDS violated right to informational privacy). Solove noted that a number of statutes also restrict disclosure of information from government records, school records, and health records, among others. Solve, *supra* note 152. *See* Privacy Act, *supra* note 120; Family Educational Rights and Privacy Act of 1974, Pub. L. 93-380, 88 Stat. 484 (codified at 20 U.S.C. §§ 1221 note, 1232g); Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (1996).

157. Roe v. Wade, 410 U.S. 113 (1973). *See also* discussion *supra* note 37 (Judge Hawkins noted in *Kincade* that the level of bodily intrusion in forced blood extraction should not be overlooked).

158. Indeed, "[p]rivacy is not merely a right possessed by individuals, but is a form of freedom built into the social structure. It is thus an issue about the common good as much as it is about individual rights. It is an issue about social architecture, about the relationships that form the structure of our society." Solove, *Digital Dossiers*, *supra* note 127, at 1116.

159. For a discussion of the "Court's failure to conceptualize privacy adequately," see Solove, *Digital Dossiers*, *supra* note 127, at 1122: "Methodologically, the Court has attempted to adhere to a unified conception of privacy. Conceptualizing privacy by attempting to isolate its essence or common denominator has inhibited the Court from conceptualizing privacy in a way that can adapt to changing technology and social practices."

160. *See supra* note 26, describing the rapid expansion in qualifying crimes for entry into a DNA database.

161. *See* LA. REV. STAT. ANN. § 15:609(A) (2004); TEX. GOV'T CODE ANN. § 411.1471 (Vernon 2003); VA. CODE ANN. § 19.2-310.2:1 (2004). In November 2004, 61.8% of California voters approved Proposition 69, mandating DNA collection from "every adult and juvenile convicted of a felony in California and from every adult arrested for certain felonies, including sex offenses, murder and voluntary manslaughter." Richard Winton & Andrew Blankstein, *Law Officials Ready to Start Expanding DNA Database*, L.A. TIMES, Nov. 4, 2004, Metro at B8; *see also* OFFICIAL VOTER

individuals who are shown to have a predisposition to violence, there may be a strong government interest in DNA testing the population at large.[162] In *Whalen*, there was a legitimate government interest in catching drug dealers and users of Schedule II drugs which authorized the storage of personal information of legal users in a computerized database.[163] There may well be a similar legitimate government interest in minimizing crime and terrorist activity on a national scale, and storage of every citizen's DNA may aid in accomplishing that objective.[164] Analogous to a drug prescription creating an opportunity to store private information, a person's visit to a doctor, or any occasion to have blood drawn, might in the future require concurrent submission to a state or national DNA database.[165] Given that the practice of storing vast quantities of personal information is becoming both endemically feasible and also inevitable, the Court should perhaps consider creating a new category of balancing test to address the informational privacy interests in personal genetic information.

INFORMATION GUIDE, CALIFORNIA STATEWIDE GENERAL ELECTION, http:/www.voterguide.ss.ca.gov/propositions/prop69-title.htm (last visited Feb. 6, 2005). The measure "also requires that starting in 2009, every adult arrested on suspicion of any felony be tested," even if they are never charged with a crime. Winton & Blankstein, *supra*. The American Civil Liberties Union is calling the measure a "vicious assault" on privacy, stating that "California now has the most draconian program for the collection, retention, and sharing of DNA data in existence anywhere in the United States." Associate Press, *ACLU Sues to Block Collection of DNA After Arrests*, L.A. TIMES, Dec. 8, 2004, Metro at B6. The ACLU is currently suing to stop the implementation of Proposition 69. *Id.*

162. *See, e.g.*, Carey Goldberg, *DNA Databanks Giving Police a Powerful Weapon, and Critics*, N.Y. TIMES, Feb. 19, 1998, at A1 ("The very existence of a DNA database smacks more of a Big Brotherish assault on privacy than the existence of the national computerized network of fingerprints. . . ."). A Boston public defender has asked when the law enforcement interest in collecting DNA should stop: "'Why not round up poor people? . . . Poor people are more likely to commit a crime, so shouldn't we have their DNA on file? . . . [W]here does it stop?'" *Id.*

163. Whalen v. Roe, 429 U.S. at 591 (record-storing program was response to concerns that "drugs were being directed into unlawful channels").

164. In fact, the Supreme Court has recently indicated a willingness to uphold local laws offering latitude to law enforcement regarding invasions of personal privacy. *See* Hiibel v. Sixth Judicial Dist. Court, 542 U.S. 177 (2004) (holding in a five–four decision that laws giving police the right to ask people their name absent individualized suspicion and jail those who do not cooperate is permissible under the Constitution). Marc Rotenberg, head of the Electronic Privacy Information Center, noted that once officers have a person's name, they can use computer databases to glean a vast amount of information by accessing linked databases: "In a modern era, when the police get your identification, they are getting an extraordinary look at your private life." *Supreme Court: Police Have a Right to Stop Anyone for No Reason at All, Demand Their Name, and Jail Them if They Refuse to Comply*, DOJGOV.NET NEWSWIRE (June 21, 2004), http://www.dojgov.net/supreme_court_privacy.htm.

165. *See* Peterson, *supra* note 96, at 1228 (discussing possibilities for compiling a universal database, such as extraction of samples from newborns or "as part of routine vaccination requirements for children entering elementary school or couples applying for marriage licenses").

VI. PROPOSAL

Given the clear direction of law enforcement toward storing genetic profiles of increasingly larger groups, the need for a judicial clarification of DNA jurisprudence is critical. I suggest in this proposal: first, an expansion of the traditional Fourth Amendment analysis to address DNA extraction and storage; and second, a legislative and administrative response to curb and respond to the rapid expansion of DNA databases. While I assume in this proposal that databanking may rapidly expand to include persons who exhibit some behavioral propensity or genetic predisposition to violence, or even the populous as a whole, the proposal is also applicable to the current system of storing profiles of convicted offenders, arrestees, and the subjects of DNA dragnets, including the 790 men in Truro, Massachusetts.[166]

A new balancing test for extraction and storage of DNA samples would aid in addressing civil liberties concerns as well as confusion over Fourth Amendment analytical tools such as the "special needs" and "totality of the circumstances" tests. While the prospect of privacy residing under a "penumbra" of constitutional rights has never fully taken root,[167] a simple Fourth Amendment inquiry seems insufficient for addressing whether taking and storing a blood sample of a particular person is constitutionally allowable.[168] Storage of genetic data for an indefinite period of time should be treated as a category distinct from searches of bags or cars or houses based on a warrant or probable cause.[169] While the Fourth Amendment does provide a convenient proxy for a balancing test, specifically with its inquiry into governmental interests (special needs) and the degree of invasion of individual privacy, it does not address the full picture.

The Court should consider creating a test that would take into account both the nature of invasion and the magnitude of access. More specifically, if a sample can be accessed in a database repeatedly and indefinitely, the extraction of such data would have to pass the balancing test for every possible occasion of access. In current form, arrestees who are later released, convicts who are exonerated, individuals who volunteer samples,

166. *See supra* notes 1–4 and accompanying text, discussing the January 2005 "DNA dragnet" in Cape Cod to solve a three-year-old murder.

167. *See supra* note 150.

168. *See supra* notes 153–54 and accompanying text.

169. *See generally* WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT (4th ed. 2004).

and even felons who complete their sentence continue to have their DNA profiles on file for any number of years, creating potential privacy invasions years down the road.[170] While the use of DNA and CODIS can indeed remarkably minimize the time needed to locate a suspect, the legal analysis of collection and storage must be cognizant of the need to protect individual privacy in a justice system where individuals are granted a presumption of innocence.[171] This intersection of rights should give the courts pause before lumping DNA extraction under the classical Fourth Amendment regime.

Coupling the judiciary trend of endorsing suspicionless searches based on governmental interest with the Bush administration's commitment to expanding the scope of CODIS and fighting the "war on terror,"[172] there is a pressing need to address the "remote possibilities" of large-scale DNA databanking. Despite the compelling argument that collecting more DNA samples will help to solve and prevent future crimes, rubber-stamping this civil liberties erosion without stringent oversight and enforcement would be reckless. The U.S. Congress should follow the trend of nations that have adopted stringent legislative oversight of state DNA databases.[173]

The first solution to appease civil libertarians and prevent snowball effects of DNA database expansion is a rigorous federal program of security standards for maintaining databases on a state level. While the DNA Act proposes guidelines for extraction and storage of samples on a federal level,[174] state DNA storage systems remain disparate.[175] A solution would include strict regulation and oversight of the protocol for extracting, storing and disposing of samples. For example, samples taken from arrestees should be disposed of if the individual is not convicted, as is the case in Australia, New Zealand, Germany, Sweden, Denmark and the

---

170. *See supra* notes 26–27 for background on federal and state legislation for increasing the list of qualifying offenses for entry into DNA databases, as well as state statutes providing for storage of samples from arrestees.

171. Professor Daniel Solove suggests that "[o]ne possible safeguard is to mandate the destruction of data after certain periods of time or, mandate the transfer of data to the judicial branch, after a certain period of time, for access only under special circumstances." Solove, *Digital Dossiers*, *supra* note 127, at 1167.

172. *See, e.g.*, Chang, *Trampling on the Bill of Rights*, *supra* note 10.

173. *See supra* notes 86–87 and accompanying text.

174. *See* DNA Analysis Backlog Elimination Act of 2000, 42 U.S.C. §§ 14135(d) (analysis of samples, including quality control); 14135a(a) (collection of DNA Samples); 14135a(b) (analysis and use of samples).

175. *See* H.R. REP. No. 106–900, pt. 1, at 8 (2000); *see also* Virna M. Samuel, *State DNA Databases and Data Bank Expansion Laws: Is it Time for California to Expand its DNA Data Base Law to Include All Convicted Felons?*, 31 W. ST. U. L. REV. 339, 340 (2004).

Netherlands.[176] The jurisdictional "hook" for federal legislation would be that for states to qualify for linkage to CODIS, security and disposal standards, at a minimum, would be mandatory.

The second step would also be legislative. Congress has made strides toward barring genetic discrimination in employment and insurance contexts.[177] The same should be done with regard to DNA in the context of crime. The DNA Act currently includes nominal punitive measures for misuses of genetic data.[178] However, more is needed. Penalties for accessing databanks should be elevated to include harsher fines and jail time—perhaps elevating the crime of improper access to a felony—for individuals who not only misuse but mishandle the samples.

In order to oversee the application of this science to law enforcement, and even employment and insurance arenas, the United States would benefit from designating a "DNA Court" to be uniquely poised to address issues related to DNA material. In addition, an administrative body, such as a Federal Bioethics Commission could advise legislators and policymakers of potential courses of action.[179] The establishment of a DNA Court would aid in monitoring the use of databases in order to safeguard against potential misuses.[180] An analogy is the congressional

176. *See supra* notes 86–87 describing some of these programs.

177. *See Protecting Against Genetic Discrimination: The Limits of Existing Laws: Hearing Before the S. Comm. on Health, Education, Labor and Pensions*, 107th Cong. 2d Sess. (2002), *available at* http://olpa.od.nih.gov/hearings/107/session2/reports/gen_discrimination.asp. A bill introduced by former Senator Thomas Daschle prohibits genetic discrimination in health insurance and employment. *Id.* According to Senator Hillary Rodham Clinton in her opening statement, "Advancements in science should help advance civilized society, not reverse our progress. And the discrimination based on genetic information would be a step backward for civilization and progress, and human dignity." *Id.* On October 14, 2003, the Senate passed S. 1053, the Genetic Information Nondiscrimination Act, by a vote of 95 to 0. The Act was designed to prohibit discrimination on the basis of genetic information with respect to health insurance and employment. S. 1053, 108th Cong. (2003) (enacted).

178. *See* 42 U.S.C. § 14135e(c) (2000). "A person who knowingly—(1) discloses a sample or result described in subsection (a) of this section in any manner to any person not authorized to receive it; or (2) obtains, without authorization, a sample or result described in subsection (a) of this section, shall be fined not more than $100,000." *Id.*

179. President Bush established The President's Council on Bioethics in 2001, by Executive Order No. 13,237, 66 Fed. Reg. 59,851 (Nov. 30, 2001). The purpose of The Council is to "advise the President on bioethical issues that may emerge as a consequence of advances in biomedical science and technology." The President's Council on Bioethics, http://www.bioethics.gov/about/executive.html. This Council, however, serves more of an advisory role to the President regarding moral and ethical dilemmas related to stem cell research, assisted reproduction, cloning, and other such issues, than it does assist in legislative development or judicial decisions. Moreover, its production of research and public reports appears to be relatively thin. Perhaps there is an independent need for a commission on bioethics dedicated to helping legislators, judges, researchers and academics resolve the very difficult issues of DNA extraction and storage in databases.

180. Yale University law professor Akhil Amar, who has advocated a mandatory national DNA database linked to birth certificates and driver's license records, has suggested the concurrent

delegation of patent claims to one court uniquely poised to decide issues of such particularity. Just as the Federal Circuit is given the responsibility of overseeing patent and trademark cases, so too should a particular court be vested with the responsibility to interpret uniquely genetic decisions.[181] The auspices of this court would extend from the criminal justice realm to cases involving questions of paternity, as well as genetic discrimination from an employer or insurer. Judges in this court would thus gain specific knowledge and become finely accustomed and attuned to the complexity of the intersection of genetic information and the law.[182] To augment this judicial initiative, a new administrative body, a Federal Bioethics Commission or perhaps a Bioethics Institute, with research and policy expertise, could play the role of a necessary oversight and advisory board to Congress and law enforcement agencies.[183] Such a board would oversee, through independent monitoring, those in charge of collecting, testing, analyzing, and storing forensic evidence.

CONCLUSION

The discovery of DNA's unique capacity for identification has been indisputably the most revolutionary law enforcement tool of the century.[184] Criminals cannot escape their own unique genetic identifiers.[185] However, as with any technological innovation, there is a danger in embracing the solution too rapidly without fully understanding the science or future implications that we may currently be unable to contemplate.[186] The Supreme Court acted in this manner in *Whalen* when embracing the use of technology—mass computerized storage of prescription records—to aid

implementation of such a court. Akhil R. Amar, *supra* note 98. "The law should . . . allow the government to search the database only for important needs, as certified by a special DNA court, whose judges would develop expertise in the uses and abuses of DNA and keep abreast of new scientific developments." *Id.* Moreover, Amar states that "there is an urgent need to legislate strong safeguards whether or not existing programs are expanded to create a universal database." *Id.*

181. A 1982 congressional decision gave authority to the Federal Circuit to assume the responsibility of the former U.S. Court of Customs and Patent Appeals. Federal Courts Improvement Act of 1982, Pub. L. 97–292, 96 Stat. 25 (Apr. 2, 1982).

182. *See supra* note 180 and accompanying text.

183. An independent body of qualified specialists would be well poised to make determinations about specific forensic and genetic issues, such as appropriate formulas to be used in court for genetic match odds.

184. *See* Rosen, *supra* note 5.

185. *See* Kimmelman, *supra* note 5.

186. Indeed, the *Whalen* Court was unable to contemplate the ease of both obtaining and exploiting private medical information. *See supra* note 119 and accompanying text. A similar fate could very well befall the information stored in DNA databases.

law enforcement interests in quelling an illicit drug market.[187] Though acknowledging that "remote possibilities" did exist for the storage system to be violated and the information to be accessed and abused, the Court did not feel that such a possibility should preclude its use.[188] This danger is concurrent with the analytical deficiencies in classifying DNA extraction under only the Fourth Amendment.

The courts are eagerly endorsing the seductive crime-fighting capacities of DNA databanking, such that they may be avoiding a necessary analysis deeper than traditional Fourth Amendment jurisprudence. The Fourth Amendment balancing test, arguably useful for storing samples of arrestees, felons on parole, and even individuals with genetic links to crime, is problematic when considering the fact that the actual privacy invasion is much more serious than the implications of a simple search. A database that can be accessed nationwide for indefinite periods of time by not only police, but also immigration services and international agencies, puts individuals of this nation and others at risk for continued encroachments on individual liberty and privacy.[189] It is critical to build safeguards into the system of database expansion now so as to mitigate the effects of *Whalen's* forecasted "remote possibilities." And perhaps a new form of balancing test would better address the reality of DNA storage as information more than simply a search.

Sasha E. Polonsky[*]

---

187. *See supra* notes 110–15 and accompanying text.

188. *See supra* notes 116–17 and accompanying text.

189. The words of Justice Louis Brandeis are now more true than ever:

> Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachments by men of zeal, well-meaning but without understanding.

Olmstead v. United States, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting).

* B.A. (2000), International Relations, East Asian Studies, Stanford University; J.D. Candidate (2006), Washington University School of Law. I would like to thank Chris Goddard, Elizabeth Hesselbach, and Tim Grasser for their valuable help in editing. With special thanks to Matthew Kriegel for editing assistance and for constant, unwavering support.