Hastings Science & Technology Law Journal

Concerns Associated with Expanding DNA Databases

by CANDICE ROMAN-SANTOS

CITE AS: 2 HASTINGS SCI. AND TECH. L.J. 267

Abstracrt

The establishment of DNA databases has been and continues to be a source f controversy. Proponents of DNA databases argue that it supports a discipline that does not rely on subjective judgments and interpretations, and expanding DNA databases will not only help to solve more crimes but also exonerate innocent people who have been wrongly convicted, ultimately reducing the need to reverse previous miscarriages of justice. Opponents of DNA databases, on the other hand, argue that there is a risk of DNA being used to the exclusion of material that might prove the innocence of the suspect. Also, the fact that DNA samples can be stored indefinitely raises concerns regarding the temptation to use those samples for new and unidentified purposes. This piece discusses the use of DNA in modern forensics, details the three largest DNA databases in the world, explains the process of obtaining a "cold hit" and the problems surrounding related probabilities and statistics that can mislead juries and courts, analyzes the problems with existing DNA database statutes in the United States (U.S.), and considers the privacy issues surrounding DNA and DNA databases.

Concerns Associated with Expanding DNA Databases

by CANDICE ROMAN-SANTOS*

I. Introduction

Deoxyribonucleic Acid (DNA) is the source of each individual's genetic makeup. The fact that each person's DNA is unique (with the exception of identical twins) and does not change over time (with the exception of mutations[1]) makes it a useful identification tool. Scientific advances have led to the creation of DNA databases that serve various purposes, including clinical research on personalized medicine, genetic testing to determine if a person has or is likely to get or be a carrier of a genetic condition, providing certainty in paternity disputes, and ancestry tests to identify ancestors who lived over 200,000 years ago. This paper will focus on the use of DNA databases by law enforcement to identify victims, missing persons, and perpetrators of crimes.

The molecular structure of DNA was discovered in 1950, and DNA typing was first applied in criminal cases in the 1980s. By the turn of the century, all fifty states had established DNA databases for individuals convicted of certain offenses.

---

* Candice Roman-Santos is a Juris Doctor candidate at the University of California Hastings College of the Law, Class of 2010. She will be graduating with Pro Bono recognition as a member of the Pro Bono Society and a Certificate in Law, Science & Health Policy from the University of California, San Francisco. She earned a Bachelor of Science degree in Integrated Science and Technology with a dual-concentration in Biotechnology and Engineering & Manufacturing from James Madison University, Class of 2001. The author would like to extend her sincerest gratitude to Lisa S. Faigman for inspiring this piece and for her continued support and friendship.

1. "Virtually every single person will have some sort of change to their DNA during their life. Changes can result from a multitude of mistakes, such as an error when DNA is replicated or through damage to DNA occurring from environmental or lifestyle factors. A DNA mutation can also be inherited." Explore DNA, What are DNA Mutations, http://www.exploredna.co.uk/what-dna-mutations.html (last visited Mar. 8, 2010).

The establishment of DNA databases has been and continues to be a source of controversy. Proponents of DNA databases argue that DNA profiles can be obtained from very small amounts of genetic data, the database supports a discipline that does not rely on subjective judgments and interpretations, and expanding the database will help to solve more crimes, exonerate innocent people who have been wrongly convicted, and reduce the need to reverse previous miscarriages of justice. Opponents of DNA databases argue that DNA analysis is not infallible, that providing personal information is governed by individual consent and should not be based on a mandatory provision, and that there is a risk that DNA will be used to the exclusion of material that might prove the innocence of the suspect. The enactment of DNA database statutes has stirred public debate about the relevant policy issues, such as: 1) who should be included, 2) what information should be included, 3) whether DNA samples should remain stored or be destroyed, and 4) whether DNA samples and records should be used for other purposes. All of these issues revolve around the single ethical concern of privacy. DNA identifies not only the person in question but also thousands of genetic conditions and predispositions to disease. Even if the DNA profiles that comprise a DNA database only include numbers that are irrelevant for other purposes, the fact that DNA samples can be stored indefinitely raises concerns regarding the temptation to use those samples for new and unidentified purposes. This risk is too great to ignore.

First, I will discuss DNA's use in modern forensics and why it is a valuable resource in criminal investigations. Second, I will discuss the three largest DNA databases in the world: 1) The Federal Bureau of Investigation's (FBI) Combined DNA Index System (CODIS), 2) The United Kingdom's (UK) National DNA Database (NDNAD), and 3) The California DNA Database. Third, I will discuss the process of obtaining a "cold hit" within CODIS and the problems surrounding related probabilities and statistics that can mislead juries and courts. Fourth, I will discuss DNA database statutes in the United States (U.S.), how legal challenges to such statutes have been resolved, the unique issues related to requiring DNA samples from mere arrestees, and the significant problems that may arise due to poor implementation of such statutes. Fifth, I will discuss the main arguments for and against expanding DNA databases. Lastly, I will focus on the issues of privacy surrounding DNA, the implications of reusing information obtained for one purpose for new and

unidentified purposes, and the concerns about function creep and misuse of personal information.

II. DNA Basics

James Watson and Francis Crick revealed a breakthrough discovery when they suggested that the structure of DNA has two helical chains each coiled around the same axis.[2] Moreover, their research suggested a possible copying mechanism for the genetic material.[3] The progression of science further revealed that human beings are 99.99% genetically similar and each individual is differentiated by 0.01% of DNA.[4] An individual's DNA can be decoded to reveal a pattern that is shared only by a genetically identical twin.[5] In addition, DNA does not change over time, except in the case of mutations.[6]

Each human being starts out as a fertilized egg with 46 chromosomes (23 chromosomes from each parent).[7] The DNA in these chromosomes is composed of pairs of molecules called "bases," and a particular order of bases that code for an observable characteristic is called a "gene."[8] A gene's position on a chromosome is called its "locus."[9] Several different arrangements of bases can form the same gene, and these variations are called "alleles."[10] DNA identification is based on how alleles of genes differ from one individual to another.[11]

III. DNA Forensics

Using DNA for identifying victims, perpetrators, missing persons, and others relies on DNA regions with short repeat units,

2. J.D. Watson & F.H.C. Crick, *Molecular Structure of Nucleic Acids*, NATURE, Apr. 25, 1953, at 737, *available at* http://www.nature.com/nature/dna50/watsoncrick.pdf.

3. *Id.*

4. AMERICAN PROSECUTORS RESEARCH INSTITUTE, FORENSIC DNA FUNDAMENTALS FOR THE PROSECUTOR 3–4 (2003).

5. OSAGIE K. OBASOGIE, PLAYING THE GENE CARD?: A REPORT ON RACE AND HUMAN BIOTECHNOLOGY 31 (Center for Genetics and Society) (2009).

6. DNA AND THE CRIMINAL JUSTICE SYSTEM: THE TECHNOLOGY OF JUSTICE 152 (David Lazer ed., The MIT Press 2004).

7. DAVID L. FAIGMAN ET AL., MODERN SCIENTIFIC EVIDENCE: FORENSICS § 2.22 (Student ed. 2008).

8. AMERICAN PROSECUTORS RESEARCH INSTITUTE, *supra* note 4, at 4–5.

9. *Id.* at 5.

10. *Id.*

11. *Id.*

called Short Tandem Repeats (STRs).[12] In 1996, the FBI established 13 STR loci as the standard for human identification, which is recognized both domestically and internationally.[13] Forensic scientists use data from the 13 loci to create a DNA profile, and the prevailing statistical probability that any two unrelated persons have identical DNA profiles at 13 loci is one in several billion.[14]

Forensic applications of DNA technology include identifying potential suspects based on an individual's DNA matching crime scene evidence, exonerating those who have been wrongly convicted of a crime, identifying crime and catastrophe victims, and establishing paternity and other familial relationships.[15]

A. How DNA is Obtained

Crime scene investigators can obtain blood, semen, urine, hairs, saliva, and other evidence, known as an evidence sample, that can yield a DNA profile.[16] A reference sample, such as blood from a suspect, is then obtained and analyzed to create another DNA profile, which is ultimately compared against crime scene evidence DNA profiles to determine whether there is a genetic match – the DNA profile obtained from the evidence sample and the reference sample are indistinguishable.[17] Genetic matches can convince the trier-of-fact in a courtroom that the two samples share a common source.

The preferred method of obtaining a reference sample is a buccal swab – using a small brush or cotton swab to collect a sample of cells from the inside surface of the cheek – because it reduces the possibility of contamination.[18] The buccal swab is an easy and rapid single-step process as opposed to other methods that often require multiple steps.[19] Each additional procedural step creates another

12. DNA Diagnostics Center, Short Tandem Repeats (STRs), http://www.forensicdnacenter.com/dna-str.html (last visited April 19, 2010).

13. *Id.*

14. OBASOGIE, *supra* note 5, at 32.

15. Human Genome Project, DNA Forensics, http://www.ornl.gov/sci/techresources/Human_Genome/elsi/forensics.shtml (last visited April 19, 2010).

16. *See* DNA Diagnostics Center, Forensic Services FAQs, http://www.forensicdnacenter.com/forensic-faqs.html (last visited April 19, 2010).

17. Charles H. Brenner, Forensic Mathematics of DNA Matching (1999), *available at* http://dna-view.com/profile.htm.

18. *Id.*

19. *See* CHANTEL MARIE GIAMANCO, COLLECTING A BUCCAL SWAB – AN ART OR A CINCH? (Human Identification Technologies, Inc.) (2009) http://www.hitdna.com/assets/pdfs%202009/Publications/Taking%20a%20Buccal%20Swab_04.2008.pdf.

opportunity for human error. Contamination can be easily avoided by collecting the sample in a low traffic area and requiring the collector to wear a mask and refrain from talking while taking the swab.[20] If a buccal swab is not an available option, other methods may be used to collect a sample of blood, saliva, semen, or other appropriate fluid or tissue from personal items (e.g., hair brush) or from stored samples (e.g., banked sperm).

B. DNA Typing

The goal of the forensic scientist is to establish the genetic profile, or "genotype," of an individual by discovering which alleles exist at strategically selected loci.[21]

In 2003, President George W. Bush created the Advancing Justice Through DNA Technology Initiative, which was a mandate on the Attorney General to improve the use of DNA in the criminal justice system.[22] The website dedicated to this initiative explains how samples obtained from crime scenes are subjected to defined processes involving biology, technology, and genetics:

> "Following collection of biological material from a crime scene or paternity investigation, the DNA is first extracted from its biological source material and then measured to evaluate the quantity of DNA recovered. After isolating the DNA from its cells, specific regions are copied with a technique known as the polymerase chain reaction, or PCR. PCR produces millions of copies for each DNA segment of interest and thus permits very minute amounts of DNA to be examined. Multiple STR regions can be examined simultaneously to increase the informativeness of the DNA test . . .
>
> The resulting PCR products are then separated and detected in order to characterize the STR region being examined. The separation methods used today include slab gel and capillary electrophoresis (CE). Fluorescence detection methods have greatly aided the sensitivity and ease of measuring PCR-amplified STR alleles. After detecting the STR alleles, the number of repeats in a DNA sequence is determined . . .

20. *Id.*

21. FAIGMAN ET AL., *supra* note 7, § 2.

22. UNITED STATES DEPARTMENT OF JUSTICE, OFFICE OF THE ATTORNEY GENERAL, ADVANCING JUSTICE THROUGH DNA TECHNOLOGY, EXECUTIVE SUMMARY (2003), http://www.justice.gov/ag/dnapolicybook_exsum.htm.

> The resulting DNA profile for a sample, which is a combination of individual STR genotypes, is compared to other samples. In the case of a forensic investigation, these other samples would include known reference samples such as the victim or suspects that are compared to the crime scene evidence.. . .If there is not a match between the questioned sample and the known sample, then the samples may be considered to have originated from different sources. If a match or 'inclusion' results, then a comparison of the DNA profile is made to a population database, which is a collection of DNA profiles obtained from unrelated individuals of a particular ethnic group."[23]

Once a genetic match is declared, a statistic is generated to convey how common or rare the matched genetic profile is in the general population (also known as the random match probability (RMP)).[24] This statistic is typically a very small number, which can help the prosecutor secure a conviction, but it may also mislead the jury in the process. This will be further explored in a later section.

IV. DNA Databases

The three largest DNA databases in the world, in decreasing order, are: 1) CODIS; 2) NDNAD; and 3) the California DNA Database.[25]

A. United States

In 1994, the Director of the FBI was authorized to establish an index of: 1) DNA identification records; 2) analyses of DNA samples recovered from crime scenes; 3) analyses of DNA samples recovered from unidentified human remains; and 4) analyses of DNA samples voluntarily contributed from relatives of missing persons.[26] The national DNA database relies on the FBI's CODIS software, which provides a central database of the DNA profiles from all public forensic DNA laboratories throughout the country.[27] The FBI

23. DNA Initiative, Steps in DNA Sample Processing, http://www.dna.gov/basics/analysis/steps (last visited Feb. 11, 2010).

24. Edward Humes, *Guilt by the Numbers*, CAL. LAW., Apr. 2009, *available at* http://www.callawyer.com/story.cfm?eid=900572&evid=1.

25. Office of the Attorney General, News Release: *Brown Announces Elimination of DNA Data Bank Backlog*, Sep. 10, 2007, *available at* http://ag.ca.gov/newsalerts/release.php?id=1464&.

26. 42 U.S.C.A. § 14132(a) (West 2009).

27. DNA Initiative, Combined DNA Index System, http://www.dna.gov/dna-databases/codis (last visited April 19, 2010).

provides CODIS software for free to all public forensic laboratories, but each laboratory is responsible for their own computer hardware and all support software.[28] CODIS is comprised of two indexes: 1) convicted offender index of DNA profiles from convicted criminals or arrestees pursuant to individual state statutes, and 2) forensic index of DNA profiles from crime scene evidence.[29] DNA samples from victims are not permitted in CODIS.[30] An individual's DNA profile must be promptly expunged from the national DNA database if his or her conviction was overturned or if the charge has been dismissed, resulted in an acquittal, or if no charge was filed.[31]

Local laboratories can maintain their own local DNA index system (LDIS) and then upload approved profiles to the state database.[32] The state DNA index system (SDIS) contains profiles from local laboratories in that state, profiles analyzed by the state laboratory itself, and profiles from convicted offenders and mere arrestees (depending on specific state statutes).[33] In addition, the FBI is responsible for obtaining samples in the federal prison system and entering those profiles into CODIS.[34] In this sense the FBI is functioning as a state laboratory.[35] Profiles from the states and the FBI are then uploaded into the national DNA index system (NDIS).[36]

The following is a graphical representation of the levels of the database.[37]

28. *Id.*

29. *Id.*

30. Chris Asplen & Lisa Hurst, Gordon Thomas Honeywell Governmental Affairs, Presentation at the National Conference for the National Center for Victims of Crime called "DNA Technology: Impact on Victims, Public Safety, and Possibilities for the Future" (Jun. 20, 2007).

31. 42 U.S.C. § 14132(a) (2009).

32. DNA Initiative, Levels of the Database, http://www.dna.gov/dna-databases/codis (last visited April 19, 2010).

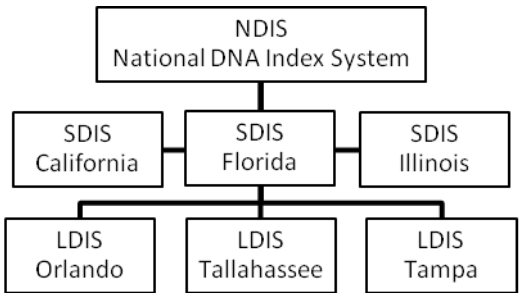
33. *Id.*

34. *Id.*

35. *Id.*

36. *Id.*

37. DNA Initiative, Levels of the Database, http://www.dna.gov/dna-databases/codis (last visited April 19, 2010).



A weekly search is conducted of all DNA profiles in the NDIS, and resulting profile matches are automatically returned to laboratories that submitted them.[38] As of April 2010, the NDIS contained over 7,940,321 offender profiles and 306,028 forensic profiles, and CODIS had produced over 107,600 hits assisting in more than 109,900 investigations.[39] The NDIS is comprised of 3 federal databases, 50 state databases, and over 70 local databases.[40]

B. United Kingdom

The NDNAD, created in 1995 in England and Wales, was the world's first DNA database.[41] Although no specific legislation established the NDNAD, legislation has since specified allowable sources of DNA samples. The NDNAD contains the largest number of DNA profiles in terms of the proportion of the population – 5.2% of the UK population as opposed to 0.5% of the U.S. population in the NDIS.[42] As of April 10, 2010, the NDNAD contained 4,856,902 DNA profiles of individuals and 354,132 DNA profiles from crime scene evidence.[43]

38. DNA Initiative, Capabilities of CODIS Software, http://www.dna.gov/dna-databases/software (last visited April 19, 2010).

39. Federal Bureau of Investigation, CODIS-NDIS Statistics, http://www.fbi.gov/hq/lab/codis/clickmap.htm (last visited April 18, 2010).

40. Tim Schellberg, Gordon Thomas Honeywell Governmental Affairs, Presentation at the ISFE Conference called "Forensic DNA Databases: A Global Update" (Nov. 10, 2009).

41. Parliamentary Office of Science and Technology, *The National DNA Database*, POSTNOTE, February 2006, *available at* http://www.parliament.uk/documents/upload/POSTpn258.pdf.

42. *Id.*

43. National Policing Improvement Agency, Statistics, http://www.npia.police.uk/en/13338.htm (last visited April 19, 2010).

The Criminal Justice and Public Order Act was passed in 1994 and authorized the creation of the NDNAD.[44] Initially, the Act allowed the police to obtain DNA samples without consent only from those charged with a recordable offense.[45] However, legislation has continually expanded police powers to take and retain DNA samples, with the goal of including "virtually the entire active criminal population" in the NDNAD.[46] For example, a 2001 law in England and Wales provided authorization to permanently retain DNA profiles and DNA samples from people who are merely arrested but subsequently acquitted or not prosecuted.[47] The scope and usage of the NDNAD has raised serious concerns and, not surprisingly, has led to legal challenges. In November 2004 the Court of Appeal ruled that the police can retain DNA samples and profiles from people who were never convicted of a crime because the relatively minor invasion of privacy is justified by the legitimate aim of preventing crime.[48] However, the European Court of Human Rights unanimously ruled in 2008 that keeping DNA samples and profiles of innocent people is unlawful and violates Article 8 of the European Convention on Human Rights (the right to respect for private and family life).[49] Despite the call to destroy the DNA records of people who are currently in the NDNAD and have been found innocent of any crime, police officers are being advised to ignore the ruling of the European Court of Human Rights.[50]

C. California

In November 2004, California voters passed Proposition 69, the DNA Fingerprint, Unsolved Crime and Innocence Protection Act.[51] Prior to the passage of Proposition 69, California law required the permanent retention of DNA samples from only convicted felons

44. Hellen Wallace, *The UK National DNA Database: Balancing Crime Detection, Human Rights and Privacy*, 7 EMBO REPORTS S26, S26 (2006), *available at* http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1490298/pdf/7400727.pdf.

45. *Id.*

46. Wallace, *supra* note 44.

47. *Id.*

48. BBC News, Police Can Keep Suspects' DNA, http://news.bbc.co.uk/2/hi/uk_news/2254053.stm (last visited April 19, 2010).

49. *Id.*

50. Ligali, Police Illegally Obtaining DNA to Create Pre-Crime Suspects, http://www.ligali.org/article.php?id=2024 (last visited April 19, 2010).

51. Office of the Attorney General for the State of California, Proposition 69 (DNA), http://ag.ca.gov/bfs/prop69.php (last visited on Nov. 29, 2009).

involving serious, violent crimes.[52] Proposition 69 amended California law to significantly expand the California DNA Database by also including people convicted of non-violent felonies (including juveniles) and individuals arrested on any felony charge, which was estimated to increase state costs by nearly $20 million annually.[53] A critique of Proposition 69 recognizes several areas where it is highly problematic. First, the law's inappropriate treatment of arrestees and suspects undermines the presumption of innocence principle.[54] Second, the law is likely to exacerbate racial bias due to pretextual behavior by law enforcement.[55] Third, the law is likely to increase human errors in DNA testing because laboratories will be overwhelmed with trying to implement the new law.[56] Fourth, the law creates the potential for misuse due to the lack of privacy protections.[57] Fifth, the substantial costs will ultimately be paid by California taxpayers.[58]

As of April 2010, the California DNA Database contained 1,251,307 offender profiles and 25,323 forensic samples, and has aided in 12,412 investigations.[59]

V. Cold Hits, Probabilities, and Access to CODIS

A *cold hit* is defined as a match between a forensic DNA profile and a known person or offender profile.[60] This means that an individual is identified solely by DNA and not through any other suspicion.[61] Matches across all 13 standard loci are known as full matches and matches across fewer than 13 loci are known as partial matches.[62] The FBI accepts partial DNA profiles of at least ten loci

52. Tania Simoncelli & Barry Steinhardt, *California's Proposition 69: A Dangerous Precedent for Criminal DNA Databases (Part I)*, 34 J.L. MED. & ETHICS 199 (2006).

53. League of Women Voters of California Education fund, Pro & Con Analysis of Proposition 69, http://ca.lwv.org/lwvc/edfund/elections/2004nov/pc/prop69.html (last visited April 19, 2010).

54. Simoncelli, *supra* note 52.

55. *Id.*

56. *Id.*

57. *Id.*

58. *Id.*

59. Federal Bureau of Investigation, CODIS-NDIS Statistics, http://www.fbi.gov/hq/lab/codis/stats.htm#California (last visited April 19, 2010).

60. OBASOGIE, *supra* note 5, at 34.

61. LINDA L. MCCABE & EDWARD R. B. MCCABE, DNA: PROMISE AND PERIL 119 (2008).

62. OBASOGIE, *supra* note 5, at 35.

for inclusion in the NDIS, and partial matches are being used more frequently as incriminating evidence.[63] If the amount of DNA recovered from a crime scene is very small or if the DNA sample recovered from a crime scene is either degraded or a mixture of DNA from many individuals, then there is often much less than 13 loci available for comparison.[64] Therefore, the statistical weight attached to a match is lower and the probability of a coincidental match is higher.[65]

Bicka Barlow, a California attorney with both a law degree and a Masters in genetics, learned that Arizona's DNA database contained two people whose genetic profiles matched at 9 loci, and filed a subpoena to learn more.[66] The resulting report revealed that, out of 65,493 offenders in Arizona's DNA database in 2005, 122 pairs of people had genetic profiles matching at 9 loci, 20 pairs matched at 10 loci, 1 pair of siblings matched at 11 loci, and 1 pair of siblings matched at 12 loci.[67] Similar assessments of DNA databases have been conducted in Illinois and Maryland.[68] Out of 220,000 profiles in the Illinois state database, 903 pairs matched at 9 or more loci, and out of 30,000 profiles in the Maryland state database, 32 pairs matched at nine loci and 3 pairs matched on all 13 loci.[69] How is this possible if the prevailing statistical probability that any two unrelated persons have identical DNA profiles at 13 loci is one in several billion?[70]

The RMP for the 122 profiles that matched at 9 loci in Arizona's DNA database was reported to be "1 in 754 million in Caucasians, 1 in 561 billion in African Americans, and 1 in 113 trillion in Southwest

63. Andrea Roth, *Safety in Numbers?: Deciding When DNA Alone is Enough to Convict*, 85 N.Y.U. L. REV. (forthcoming 2010) (manuscript at 7); OBASOGIE, *supra* note 5, at 35.

64. Linda Geddes, *Unreliable Evidence? Time to Open Up DNA Databases*, NEW SCIENTIST, Jan. 6, 2010, *available at* http://www.newscientist.com/article/mg20527424.700-unreliable-evidence-time-to-open-up-dna-databases.html?full=true.

65. *Id.*

66. Jon Jefferson, *Cold Hits Meet Cold Facts: Are DNA Matches Infallible?*, TRANSCRIPT, Spring 2008, at 32.

67. *Id.* at 32–33.

68. Linda Geddes, *Unreliable Evidence? Time to Open Up DNA Databases*, NEW SCIENTIST, Jan. 6, 2010, *available at* http://www.newscientist.com/article/mg20527424.700-unreliable-evidence-time-to-open-up-dna-databases.html?full=true.

69. *Id.*

70. OBASOGIE, *supra* note 5, at 32.

Hispanics.[71] Therefore, the discovery of even one match at 9 loci in a database of only 65,493 profiles is alarming. However, this only becomes a cause for concern if the size of the database is conflated with the number of comparisons being made to find a match.[72] Charles Brenner, a forensic mathematics consultant, explains:

> "There are two separate multiplicative factors that the naïve tend to overlook when considering the number of possible 9-locus matches from a collection of profiles such as the Arizona data: 1) the factor, equal to one-half the size of the sample, by which the number of *pairs* exceeds the size of the sample, and 2) the combinatorial factor – 715 above- representing the number of different 9-locus selections from 13, each of which is an opportunity for two selected individuals to have a 9-locus match."[73]

These two factors can be better understood by analyzing "the birthday problem," which asks how many people you need to have at a party so that there is more than a 50 percent chance that two of them will share the same birthday?[74] Most people believe the answer to be 183 – the smallest whole number larger than 365/2 – when the correct answer is actually 23.[75] Having 23 people in a room yields 253 different ways of pairing two people together, which provides many possibilities of finding a pair with the same birthday.[76]

The 65,493 profiles in Arizona's DNA database creates 2,144,633,778 distinct pairs, and though there is only one way to match all 13 loci, there are 715 distinct combinations of nine items out of thirteen.[77] Assuming that the RMP of a 9 loci match is "1 in 754 million," then the expected number of 9 loci matches would be 2,034, which reveals that RMPs are even smaller than the theoretical estimates.[78] In reality, however, each genetic profile has its own RMP

71. David H. Kaye, *Trawling DNA Databases for Partial Matches: What is the FBI Afraid Of?*, 19 Cornell J.L. & Pub. Pol'y 145, 154 (2009).

72. Kaye, *supra* note 71.

73. CHARLES BRENNER, ARIZONA DNA, DATABASE MATCHES (2007), *available at* http://dna-view.com/ArizonaMatch.htm.

74. Scott Simon, "Math Guy: The Birthday Problem," NPR (2005), *available at* http://www.npr.org/templates/story/story.php?storyId=4542341.

75. *Id.*

76. *Id.*

77. Kaye, *supra* note 71, at 157.

78. *Id.*

within each population group, and more research is required to determine whether RMPs are accurate or either too high or too low.[79]

The RMP is only relevant in assisting the jury measuring the probative value of a given case's circumstantial evidence.[80] It answers the question: How rare is the identified genetic profile in the general population?[81] However, because cold hits represent a query for matches among thousands of DNA profiles rather than for a specific suspect, many statisticians argue that the relevant question is: What is the likelihood that the database will spit out an innocent person's name?[82] Sir Alec Jeffreys, the original inventor of DNA typing, has warned that when extremely large databases (such as CODIS and the NDNAD) undergo large numbers of exploratory searches, even exceptionally rare matches will occur.[83] In a 1996 report titled "The Evaluation of Forensic DNA Evidence," the National Research Council concluded that the database match probability should be used to explain the significance of a cold hit DNA match.[84] However, the FBI has ignored this recommendation.[85]

There are a few possible reasons why the DNA database studies conducted in Arizona, Illinois, and Maryland yielded such high numbers of matching pairs given the relatively low number of profiles that comprised each database. One possible reason is duplicate entries of the same profile, for example if an individual's DNA profile was entered once under his or her real name and again under his or her alias.[86] A second possible reason is that the assumptions about the frequency of alleles in populations, such as by race, ethnicity, or geography, are incorrect.[87] A third possibility is that there are large numbers of relatives in the database, who are more likely than non-

79. *Id.* at 158.

80. Kaye, *supra* note 71, at 150–51.

81. Edward Humes, *Guilt by the Numbers*, CAL. LAW., Apr. 2009, *available at* http://www.callawyer.com/story.cfm?eid=900572&evid=1.

82. *Id.*

83. MICHAEL LYNCH ET AL., TRUTH MACHINE: THE CONTENTIOUS HISTORY OF DNA FINGERPRINTING 145 (2008).

84. Edward Humes, *Guilt by the Numbers*, CAL. LAW., Apr. 2009, *available at* http://www.callawyer.com/story.cfm?eid=900572&evid=1 (citing NATIONAL RESEARCH COUNCIL, THE EVALUATION OF FORENSIC DNA EVIDENCE (National Academy of Sciences) (1996)).

85. *Id.*

86. Linda Geddes, *Unreliable Evidence? Time to Open Up DNA Databases*, NEW SCIENTIST, Jan. 6, 2010, *available at* http://www.newscientist.com/article/mg20527424.700-unreliable-evidence-time-to-open-up-dna-databases.html?full=true.

87. *Id.*

relatives to have similar DNA profiles.[88] The real issue stems from the fact that while studies similar to the Arizona DNA database study raise serious concerns about the effectiveness of DNA databases and the accuracy of RMPs, state and federal governments are resisting calls to fully investigate the existence of numerous database matches across 9 or more loci.[89]

An Arizona judge barred Barlow from circulating the report on Arizona's multiple database matches, and the FBI has threatened to bar crime labs from participating in the national DNA database if they share database information with anyone outside of law enforcement.[90] Also, a California judge has denied Barlow access to data about California's DNA database.[91] The problem is that "cold hit matches that occur *within databases* do not reflect the same odds as finding a match *within entire populations*."[92]More recently, the California Supreme Court heard a case in which the prosecution presented evidence that the odds that a random person unrelated to the defendant could have left the evidence at the crime scene are one in 1,000,000,000,000,000,000,000 (sextillion).[93] Because the world's total population is only about seven billion, this was tantamount to saying that the defendant was guilty. The court held that the evidence was proper, reasoning that the calculation was a rarity statistic rather than a calculation reflecting the number of potential suspects excluded through the database search.[94]

Access to DNA databases is critical to testing the accuracy of claims that 13 loci DNA profiles are so rare that they are effectively unique in the population.[95] Assessing the rarity of a trait requires knowledge about the frequency of that trait in a given population. In 2009, 41 scientists and defense lawyers signed a letter to the FBI demanding access to CODIS so that they can test the underlying assumptions behind the DNA database statistics that are often used

88. *Id.*

89. Jefferson, *supra* note 66, at 33; Edward Humes, *Guilt by the Numbers*, CAL. LAW., Apr. 2009, *available at* http://www.callawyer.com/story.cfm?eid=900572&evid=1.

90. *Id.*

91. *Id.*

92. OBASOGIE, *supra* note 5, at 35 (emphasis in original).

93. People v. Nelson, 185 P.3d 49 (2008).

94. *Id.* at 66.

95. Roth, *supra* note 53, at 11.

to justify convictions.[96] The FBI has denied this and earlier requests for access to CODIS on privacy grounds.[97] However, the signatories to the letter specifically requested the database "as an electronic file consisting of the complete genetic profiles . . . of every individual in the database with identifying information removed."[98] The privacy issues deal primarily with retention and potential misuse of DNA samples and not the genetic profiles that make up CODIS. If personal identifiers are removed and only anonymous genetic profiles are released, the potential threat to individuals becomes non-existent.

Those opposed to granting researchers access to CODIS also argue that doing so constitutes a breach of informed consent – the right to consent or refuse to take part in research.[99] However, informed consent regarding receipt of medical treatments or participation in research involving human subjects involves "the rights to be free from intentional bodily harm, from offensive touching or intrusion, from unnecessary confinement and physical restraint, and from serious and reasonable emotional distress."[100] These rights are not implicated when DNA samples are legally compelled, and especially when releasing this information will be "used solely to ensure that the very system that justifies this compulsion is working as it should."[101] Therefore, lack of individual consent to release anonymous genetic profiles to researchers is an insufficient reason to block access to CODIS.

The DNA Identification Act of 1994, which is the legislation that established the NDIS, explicitly allows database records to be made available "for a population statistics database, for identification research and protocol development purpose, or for quality control purposes" as long as all personally identifiable information is first removed.[102] President Obama is also concerned with scientific integrity, stating in a March 9, 2009, memorandum to the heads of executive departments and agencies that "if scientific and

96. [No author], *Time for Full and Frank Data Disclosure,* New Scientist, Jan 6, 2010, *available at* http://www.newscientist.com/article/mg20527423.500-time-for-full-and-frank-data-disclosure.html.

97. *Id.*

98. Keith Inman, Criminal Justice Administration department at California State University, Hawyard, Presentation at University of California Hastings College of the Law called "The Scientific Basis of Forensic DNA" (Nov. 10, 2009).

99. Kaye, *supra* note 71, at 169.

100. *Id.* at 170.

101. *Id.* at 169–70.

102. 42 U.S.C. A. §§ 14132(a), 14132(b)(3)(D) (West 2010).

technological information is developed and used by the Federal Government, it should ordinarily be made available to the public.[103] In addition, a National Research Council report openly criticized how insular forensic science is, detached from the conventional norms of the scientific process.[104] The fact that providing researchers with access to CODIS is authorized by Congress and supported by the President and the National Research Council, combined with the failed arguments of privacy and consent to block access, makes the FBI's reluctance to do so seem like they have something to hide. The use of DNA evidence in the criminal justice system is a science. One of the fundamental maxims in science is that hypotheses must be tested, and open access to data will allow for the independent scientific scrutiny that normally occurs during the peer review and publication process.

Allowing researchers to access CODIS will facilitate future studies to determine whether the number of matches arising from the evaluation of individual state DNA databases can be reconciled with the fundamental assumptions that scientists rely upon when calculating the frequency of genetic profiles. More transparency is essential to keeping the system fair and honest, and to preventing innocent people from being sent to prison.[105] Proponents of DNA databases argue that DNA typing is accurate and provides conclusive evidence of guilt, as supported by the DNA statistics presented to a jury in a criminal trial. The problem is that DNA statistics can be misleading due to such things like failing to consider the potential for error, failing to consider relatives, improperly analyzing a mixed sample containing DNA from more than one individual, and statistical fallacies. The impact of such misunderstanding can be quite grave, considering that a defendant's life and liberty are on the line. The call to expand the DNA database – given the problems associated with how the database is used in our criminal justice system – makes the serious privacy implications associated with such expansion more controversial because it is unclear whether the interest of justice is actually being served.

103. Barack Obama, Memorandum for the Heads of Executive Departments and Agencies, Mar 9, 2009, *available at* http://www.whitehouse.gov/the_press_office/Memorandum-for-the-Heads-of-Executive-Departments-and-Agencies-3-9-09/.

104. D.E. Krane et. al., *Time for DNA Disclosure*, 326 Science 1631 (Dec. 18, 2009).

105. Edward Humes, *Guilt by the Numbers*, CAL. LAW., Apr. 2009, *available at* http://www.callawyer.com/story.cfm?eid=900572&evid=1.

VI. DNA Database Statutes in the United States

Though common themes exist, all 50 states and the federal government have enacted separate statutes creating DNA databases.[106] As of January 2009, all 50 states have statutes requiring DNA samples to be collected from convicted felons, but they differ based on state-qualifying offenses.[107] For example, while 47 states require DNA samples from all convicted felons, the statutes of 40 states apply retroactively to those already incarcerated prior to the statutes' effective dates and 32 states require DNA samples from adults and juveniles alike.[108] Additionally, 37 states have statutes requiring DNA samples from those convicted of sex-crime misdemeanors, 5 of which also require DNA samples from those convicted of numerous other misdemeanors as well.[109]

In efforts to expand DNA databases, 21 states have statutes requiring DNA samples from those arrested for murder or sex crimes, 19 of which additionally require DNA samples from those arrested for burglary.[110] The federal government and California, along with 10 other states, require DNA samples from those arrested for any felony.[111] If charges are dropped, dismissed, or if the arrestee is found not guilty, 12 states provide expungement of the DNA profile upon request and 8 states expunge the DNA profile automatically.[112] Minnesota is an exception because state legislation provides for automatic expungement of a DNA profile upon a finding of not guilty and expungement upon request of a DNA profile if the charges were dismissed or dropped.[113]

In early 2009, pursuant to the 2005 DNA Fingerprint Act, the federal government approved a plan to collect DNA samples from

106. *Validity, Construction, and Operation of State DNA Database Statutes*, 76 A.L.R.5D 239, at § 2(b) (2009); Tim Schellberg, Gordon Thomas Honeywell Governmental Affairs, Presentation at ISFE Conference: Forensic DNA Databases: A Global Update (Nov. 10, 2009).

107. DNA Resource.com, State DNA Database Laws Qualifying Offenses, http://www.dnaresource.com/documents/statequalifyingoffenses2009.pdf (last visited Nov. 30, 2009).

108. *Id.*

109. *Id.*

110. DNA Resource.com, State Laws for Arrestee DNA Databases, http://www.dnaresource.com/documents/ArresteeDNALaws-2009.pdf (last visited Nov. 30, 2009).

111. *Id.*

112. *Id.*

113. DNA Resource.com, State Laws for Arrestee DNA Databases, *supra* note 110.

undocumented immigrants, but the Immigration and Customs Enforcement (a division of Homeland Security) was not collecting DNA from detained immigrants as of August 2009.[114] Those who oppose this law argue that most undocumented immigrants are held for suspected violations of civil law and therefore should not be entered into a criminal database, and collecting DNA from immigrants does not serve a legitimate law enforcement purpose because most are hard-working people.[115]

A. Legal Challenges

Several courts have held that enforcing a state DNA database statute does not violate the Eighth Amendment prohibition of cruel and unusual punishment, nor does it violate the Fifth Amendment right against self incrimination because DNA samples are not considered to be testimonial in nature.[116] Courts have also upheld DNA database statutes that are intended or permitted to apply to persons convicted prior to the enactment of the relevant database statute.[117]

Regarding the Fourth Amendment, several courts have expressed the view that a state's DNA database statute does not violate the Fourth Amendment rights of those persons subject to the statute, reasoning that such an intrusion is reasonable in light of the need to ensure public safety and prisoners' diminished expectation of privacy.[118] The U.S. Supreme Court has denied certiorari in an Eleventh Circuit case holding that Georgia's DNA database statute does not violate the Fourth Amendment of the Constitution because the public safety outweighed the minor intrusion involved in taking prisoners' saliva samples, given the prisoners' reduced expectation of privacy in their identities.[119] Similarly, the Court has also denied certiorari in a Second Circuit case holding that New York's DNA database statute does not violate the Fourth Amendment of the

114. Emily Witt & Ben Protess, *DNA Testing of Detained Immigrants Easier Said Than Done*, PROPUBLICA, Aug. 5, 2009, http://www.propublica.org/feature/dna-testing-of-detained-immigrants-easier-said-than-done-805.

115. *Id.*

116. *Validity, Construction, and Operation of State DNA Database Statutes*, 76 A.L.R.5D 239, at §§ 3 and 11 (2009).

117. *Id.* at § 22.

118. *Id.* at §§ 10, 14–16 (no violation under traditional Fourth Amendment analysis, special needs exception, and prisoners' reduced privacy exception).

119. Boulineau v. Donald, 546 U.S. 820 (2005); *see* Padgett v. Donald, 401 F.3d 1273 (11th Cir. 2005).

Constitution because it falls within the "special needs" exception – the notion that collecting DNA samples from prisoners is beyond the normal need for criminal law enforcement, making the warrant and or probable cause requirements of the Fourth Amendment impracticable or irrelevant.[120] By denying certiorari, the U.S. Supreme Court is implicitly affirming the rulings of the Second and Eleventh Circuits. This will make it more challenging for those opposing DNA database statutes on Fourth Amendment grounds.

Even when a relatively clear Fourth Amendment violation results in an individual's DNA profile being placed in the DNA database, courts may nonetheless choose not to apply the exclusionary rule. Nine years ago, Earl Whittley Davis was a shooting victim whose DNA profile was subsequently uploaded into CODIS even though he had done nothing wrong.[121] This victim then became the subject of a cold case hit for a murder that occurred in 2004.[122] Although the Maryland District Court found that crime control was a generalized interest that did not outweigh Davis' privacy when placement of his DNA profile in CODIS was not in response to a warrant or to an applicable statute, the Court held that the DNA evidence was nonetheless admissible.[123] The Court reasoned that placement of Davis' profile in CODIS was not reckless, flagrant or systematic, that exclusion would result in only marginal deterrence, if any, and that any deterrent effect would be greatly outweighed by the cost of suppressing "powerfully inculpatory and reliable DNA evidence."[124] This case should lead people to fear that utilizing such practices to expand the DNA database would open a backdoor to population-wide data banking.[125]

120. Nicholas v. Goord, 549 U.S. 953 (2006); *see* Nicholas v. Goord, 430 F.3d 652 (2d Cir. 2005).

121. Fourth Amendment.com, Cold Case Hit of DNA from a Shooting victim 9 Years Ago was Unreasonable Seizure, but Exclusionary Rule Not Applied (2009), http://fourthamendment.com/blog/index.php?blog=1&title=d_md_cold_case_hit_of_dna_from_a_shootin&more=1&c=1&tb=1&pb=1 (last visited April 19, 2010).

122. *Id.*

123. United States v. Davis, RWT 07-0199, 2009 U.S. Dist. LEXIS 83864, at *87 (D. Md. September 15, 2009).

124. United States v. Davis, RWT 07-0199, 2009 U.S. Dist. LEXIS 83864 at *98-100.

125. United States v. Davis, RWT 07-0199, 2009 U.S. Dist. LEXIS 83864 at *90 (citing Edward J. Imwinkelried & D.H. Kaye, *DNA Typing: Emerging or Neglected Issues*, 76 Wash. L. Rev. 413 (2001)).

B. The Issue of Including Arrestees in a DNA Database

The U.S. Constitution has not been held to necessarily preclude the inclusion of arrestees in a DNA database.[126] However, reasons for upholding the requirement of collecting DNA samples from convicts cannot necessarily be used to justify requiring the collection of DNA samples from arrestees. For example, the consequences of an arrest are not as severe as those of a conviction, and an arrest is not the equivalent of guilt. Therefore, arrestees should not have a reduced privacy interest. Some arrestees have not been convicted of any crime, nor may they ever be, and if the police reasonably suspect an individual arrestee then they can and should seek a warrant for a DNA sample.[127]

Another issue regarding taking DNA samples from arrestees is expungement. Critics argue that the databank should bear the responsibility of ensuring that DNA samples that do not belong in the database are removed, however most states that require collection of DNA samples from arrestees make the individuals responsible for ensuring the expungement of their DNA profiles and the destruction of their DNA samples.[128] For example, an individual who is eligible for expungement in California would have to send a formal request to the trial court where he or she was arrested, the California Department of Justice's DNA Laboratory, and the prosecuting attorney, and no appeal process is available if the court denies the request.[129]

The Orange County District Attorney's Office has begun offering to drop charges for mere arrestees of nonviolent misdemeanors in exchange for a DNA sample.[130] Critics argue that this practice is tantamount to pressuring people who have not been convicted of any crime to give the government a DNA sample, and that people will do so to avoid a potentially prolonged and challenging relationship with the legal system even if they are truly innocent.[131]

---

126. DNA AND THE CRIMINAL JUSTICE SYSTEM, *supra* note 6, at 258.

127. Simoncelli, *supra* note 52, at 204.

128. *Id.*

129. *Id.*

130. Tami Abdollah, *Arrested in O.C.? A DNA Sample Could Buy Freedom*, L.A. TIMES, Sept. 17, 2009, *available at* http://articles.latimes.com/2009/sep/17/local/me-oc-dna17.

131. Abdollah, *supra* note 130.

The UK NDNAD contains almost five million samples, and almost one million of them are known to be of innocent people.[132] The UK has implemented an official policy of arresting people for the sole purpose of obtaining their DNA, which reflects a system that presumes guilt even before an actual crime has been committed.[133] Though such a practice violates the American principle of an individual being presumed innocent until proven guilty, the U.S. Supreme Court and state Supreme Courts may consider pretextual police behavior acceptable, effectively giving law enforcement carte blanche authority to expand DNA databases.[134]

C. Consequences of Poor Implementation

Poor implementation of a state DNA database statute can lead to significant problems. One example is Maryland's backup system for its DNA database involving downloading the database onto a tape each evening, which an employee takes home and returns the next morning.[135] Not only does this system make sensitive information vulnerable to unauthorized access, but if anything should happen to the main computer system or hard drive, critical data would be lost and not easily recovered.[136] A second example is the fact that approximately 50,000 felons have been released from Illinois prisons or county probation without submitting DNA samples as required by law due to delays in the law's implementation.[137] A third example is the recent disclosure that an audit of Wisconsin's statewide DNA database revealed that the profiles of at least 12,000 felons were missing, 70 percent of which are believed to still be in custody or

132. Ligali, Police Illegally Obtaining DNA to Create Pre-Crime Suspects, http://www.ligali.org/article.php?id=2024 (last visited April 19, 2010).

133. *Id.*

134. *See* Whren v. United States, 517 U.S. 806 (1996) (holding that traffic stops for violation of a traffic law is valid even if the officer would not have stopped the motorist except for some other law enforcement objective); *see* Atwater v. City of Lago Vista, 532 U.S. 318 (2001) (holding that the Fourth Amendment does not forbid a warrantless arrest for minor criminal offense); *see* Washington v. State, 653 So.2d 362 (Fla. 1994) (holding that the police may trick suspects into giving DNA samples for one investigation by asking them to give DNA samples for unrelated investigations).

135. Ralph Brave, *DNA To Go*, BALT. CITY PAPER, Jul. 28, 2004, *available at* http://www.citypaper.com/news/story.asp?id=8628.

136. *Id.*

137. Megan Twohey, *DNA Law Misses 50,000 Felons Released in Illinois*, CHICAGO TRIBUNE, Sept. 1, 2009, *available at* http://www.chicagotribune.com/news/local/chi-dna-crack-in-law-01-sep01,0,1218869.story.

under state supervision.[138] A suspect in a string of murders that occurred from 1986 to 2007 was a convicted felon whose DNA profile should have been in the state's database, and the police might have focused on him sooner if it had been. These examples demonstrate how effective implementation is critical to realizing the public safety goals that a DNA database statute is meant to achieve.

VII. Pros and Cons of DNA Databases

DNA may be more objective and accurate than other forensic disciplines that rely heavily on subjective judgments and interpretations, but DNA is not infallible and can be corrupted by environmental factors (e.g., heat, sunlight, bacteria) and is subject to human error or fraud in comparing samples taken from suspects with samples removed from a crime scene.[139] Proponents claim that a DNA database is not intended to replace conventional criminal investigations but to complement them by identifying potential suspects sooner who can then be further investigated using more conventional means.[140] However, there is a serious risk that evidence tending to prove the innocence of a suspect may be overlooked in light of DNA evidence because people will be blinded by the science.[141] Even though forensic DNA has been used to exonerate people who have been wrongly convicted, it would be ironic if the same evidence is used to create injustices of its own.[142]

Advocates of DNA databases claim that obtaining a DNA sample for a government database does not raise privacy concerns because the procedure for taking a DNA sample is less invasive than that required for taking blood.[143] A number of complications may arise during the blood collection process, including fainting, incorrect needle insertion, bruising, and excessive bleeding.[144] Another argument to counter privacy concerns is that personal information is already held by groups in the private sector, and if people can trust

138. Assoc. Press, *DNA Profiles of Many Felons are Missing in Wisconsin*, N.Y. TIMES, Sep. 16, 2009, *available at* http://www.nytimes.com/2009/09/17/us/17wisconsin.html?_r=1.

139. THE INT'L DEBATE EDUC. ASS'N, THE DEBATABASE BOOK: A MUST HAVE GUIDE FOR SUCCESSFUL DEBATE 84 (4th ed. 2009).

140. *Id.* at 85.

141. *Id.*

142. *Id.* at 85–86.

143. THE INT'L DEBATE EDUC. ASS'N, *supra* note 139, at 85.

144. Health Sciences Division, Austin Community College, *Complications in Blood Collection* 66 (2004), *available at* http://www.austincc.edu/health/phb/documents/PHBLec8ComplicationsinBloodCollectionSum04.pdf.

the private sector then they should be able to trust the government.[145] However, the invasiveness of the database and source of privacy concerns is the fact that DNA samples are retained.[146] Individuals who provide their own personal information to the private sector do so voluntarily, and usually in exchange for a service (e.g., insurance brokers require an extensive medical history of their clients before approving insurance coverage, mortgage lenders demand a full credit record of each applicant before approving loans).[147] DNA database statutes make providing a DNA sample mandatory while offering nothing in return.[148] In addition, American discontent with political leaders, lack of faith in the political system, poor government performance, and the overall condition of the nation are key factors behind public distrust of the government.[149] Thus, arguments that the government should be entrusted with private and personal information may fall on deaf ears.

Supporters of expanding the DNA database argue that to suppress DNA usages because they might become abuses is akin to arguing that we should not allow rapid trains to be built because they might be used to transport victims to concentration camps.[150] There are many uses of DNA that do not raise significant concerns, such as creating a DNA profile of a suspect after he or she has been identified, but obtaining and retaining DNA profiles and samples from innocent people is not one of them. With government efforts to expand the national DNA database, critics worry that the U.S. is becoming a genetic surveillance society.[151] Benjamin Keehn, a public defender in Boston, argued on PBS NewsHour that "if we are going to take DNA from prisoners because they are at-risk [of committing crimes in the future], why shouldn't we take DNA from teenagers, from homeless people, from Catholic priests, from any subgroup of society that someone is able to make a statistical argument of being

145. *Id.*

146. *Id.*

147. *Id.*

148. *Id.*

149. THE PEW RESEARCH CENTER FOR THE PEOPLE & THE PRESS, HOW AMERICANS VIEW GOVERNMENT: DECONSTRUCTING DISTRUST, 13 (1998), http://people-press.org/reports/pdf/95.pdf.

150. DNA AND THE CRIMINAL JUSTICE SYSTEM, *supra* note 6, at 198.

151. Solomon Moore, *F.B.I. and States Vastly Expand DNA Databases*, N.Y. TIMES, Apr. 18, 2009, *available at* http://www.nytimes.com/2009/04/19/us/19DNA.html?_r=1.

at-risk?"[152] As time passes, science advances, and the scope and usage of DNA databases grow, the line being drawn between what is and is not acceptable will encroach more and more on individual privacy.

VIII. Privacy Implications of DNA

Privacy is not threatened by the means of obtaining DNA samples, but rather the information inherent in DNA and the individual's lack of control over such information.[153] There are few subject areas more personal and more likely to implicate privacy interests than that of an individual's health or genetic make-up.[154] The concern is that as the uses for and access to the DNA database increases, the threat to privacy also increases.[155]

DNA samples have been analogized to medical information stored on a computer disk because both can be "read" by the application of technology.[156] Though medical information may be strongly correlated with particular diseases, DNA is inherently linked to one person (except in the case of identical twins).[157] An individual's medical information may change over the course of his or her lifetime (e.g., people being diagnosed with diabetes, asthma, high cholesterol, or heart disease well into adulthood), but with the exception of mutations, DNA does not change over time.[158] An individual's medical information may have implications for others (e.g., a virus infection has implications for others as the infected person may get others sick), just as DNA has implications for individuals other than the person from whom the information was derived.[159] However, the implications of medical information are not as serious as those of DNA, which involve invading the privacy of a person's family when no family member is guilty of any wrongdoing. Close relatives such as parents, siblings and children share about fifty

152. Christine Rosen, *Liberty, Privacy, and DNA Databases*, THE NEW ATLANTIS, Spring 2003, at 37, *available at* http://www.thenewatlantis.com/docLib/TNA01-Rosen.pdf.

153. DNA AND THE CRIMINAL JUSTICE SYSTEM, *supra* note 6, at 226.

154. Norman-Bloodsaw v. Lawrence Berkeley Lab., 135 F.3d 1260, 1269 (9th Cir. 1998).

155. *See* KRISTINA STALEY, THE POLICE NATIONAL DNA DATABASE: BALANCING CRIME DETECTION, HUMAN RIGHTS AND PRIVACY 36 (2005), *available at* http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/NationalDNADatabase.pdf.

156. DNA AND THE CRIMINAL JUSTICE SYSTEM, *supra* note 6, at 137–38.

157. *Id.* at 152.

158. DNA AND THE CRIMINAL JUSTICE SYSTEM, *supra* note 6, at 152.

159. *Id.* at 151–152.

percent of each other's genetic variants and STR lengths, and more distant relatives such as uncles, aunts, nephews, nieces, grandparents, grandchildren, and half-siblings share about twenty-five percent of each other's DNA variants.[160] Thus, using partial matches to identify potential suspects radically expands the power and purpose of DNA databases, implicating a number of people who may have nothing to do with the original crime.

There are substantial differences between DNA profiles and ordinary fingerprints and it trivializes DNA to call a DNA profile a genetic fingerprint.[161] Fingerprints are two-dimensional representations of the physical attributes of fingertips and provide no information about a person other than identity.[162] In addition to providing an individual's identity, DNA can also provide medical characteristics, physical attributes, who the individual may be related to, and other personal information that, in the wrong hands, can perpetuate discriminatory practices.[163] Whereas a latent fingerprint provides a fixed amount of information, all of which is used by the forensic scientist, a DNA sample provides a wealth of information and the forensic scientist has substantial control over the amount of information to be obtained from the sample.[164] DNA is more probative than fingerprints because unlike fingerprints which establish that a suspect was present at a location and does not automatically imply guilt, it is more difficult to advance innocent reasons for the presence of DNA in the form of bodily fluids.[165] These differences are relevant to how DNA databases should be used and maintained, especially considering the privacy concerns unique to DNA.

Proponents of DNA databases claim that DNA profiles consist merely of "junk DNA" that is incapable of revealing information about an individual's genetic make-up or health.[166] However, a British team has discovered that the standard DNA profile contains a

160. Henry T. Greely et al., *Family Ties: The Use of DNA Offender Databases to Catch Offenders' Kin (Part I)*, 34 J.L. MED. & ETHICS 248, 251–252 (2006).

161. DNA AND THE CRIMINAL JUSTICE SYSTEM, *supra* note 6, at 173.

162. *Id.*

163. NATIONAL RESEARCH COUNCIL, DNA TECHNOLOGY IN FORENSIC SCIENCE, at 113 (National Academy of Sciences) (1992), *available at* http://www.nap.edu/openbook.php?isbn=0309045878 (last visited Apr. 19, 2010).

164. *Id.* at 112.

165. NATIONAL RESEARCH COUNCIL, DNA TECHNOLOGY IN FORENSIC SCIENCE, *supra* note 163, at 112.

166. David Concar, *What's in a Fingerprint*, NEW SCIENTIST, May 5, 2009, at 9.

subtle signature which can be linked to a person's susceptibility to type 1 diabetes.[167] This research was buried in an academic paper, did not comment on the implications for forensic science, and has been overlooked by the forensic and legal communities.[168] DNA forensic testing relies on the principle that DNA profiles are only useful for identification, which is how people justify storing DNA profiles on law enforcement computers because they do not infringe anyone's medical privacy.[169] Sir Alec Jeffreys was a member of the research team that made this discovery, and he predicted that "further troubling links between DNA fingerprints and disease will emerge as scientists probe the completed draft of the human genome."[170]

The U.S. has failed to employ comprehensive privacy regulations that would prevent the government from sharing DNA profiles in a DNA database with other groups, such as insurance companies, employers, or academia.[171] DNA database statutes can be grouped into broad categories based on authorized uses of both DNA profiles and raw DNA samples: 1) statutes that allow access to DNA for non-law enforcement purposes, 2) statutes that allow access to DNA information to public officials other than law enforcement, 3) statutes that allow law enforcement to use DNA evidence for purposes other than identification, and 4) statutes that do not require expungement of DNA records upon reversal.[172] Some state laws, such as Massachusetts, Louisiana and North Carolina, include a vague, open-ended authorization that allows the database to be used for "other humanitarian purposes."[173] Alabama's statute explicitly authorizes the creation and use of a DNA population statistical database "to provide data relative to the causation, detection and prevention of disease or disability," as well as to assist in educational or medical research.[174] Mississippi's law authorizes the Mississippi Crime Laboratory to determine any restrictions, and Utah's law provides

167. *Id.*

168. *Id.*

169. *Id.*

170. Christine Rosen, *Liberty, Privacy, and DNA Databases*, THE NEW ATLANTIS, Spring 2003, at 37, 37, *available at* http://www.thenewatlantis.com/docLib/TNA01-Rosen.pdf.

171. Jeffrey Rosen, *Genetic Surveillance for All*, SLATE, Mar. 17, 2009, http://www.slate.com/id/2213958/.

172. DNA AND THE CRIMINAL JUSTICE SYSTEM, *supra* note 6, at 176.

173. *Id.*; Simoncelli, *supra* note 52, at 203.

174. Simoncelli, *supra* note 52, at 203.

insurance companies, psychologists, and other third parties with access to information in the state DNA database.[175]

Some argue that creating a whole-population database is logical because a larger database is more useful than a smaller one, and it has the added effect of purging racial bias from the system, thereby avoiding criticisms of discrimination that result from selective sampling of the population.[176] However, this alone is insufficient to justify a whole-population database, and for many the critical factor is not merely the creation of a whole-population database of genetic profiles, but the retention of all of the DNA samples used to generate the genetic profiles. The potential for the government to use the DNA samples for a purpose not originally conceived of at the time that the DNA sample was obtained is frightening. The problem of function creep will be explored in the next section.

The United States, Germany, and other countries have been guilty of implementing national programs in the name of eugenics that clearly violated human rights.[177] The eugenics movement lost credibility after the rise of Nazism in the 1930s, but re-emerged as a scientific endeavor and social issue following the advent of biotechnology in the 1970s.[178] Science fiction literature and movies have dealt with the issue of "new eugenics" - the use of technology to make directed changes to human evolution.[179] These works convey the danger that the ability to manipulate an individual's genetic makeup will result in removing physical and behavioral traits not desired by society as a whole.[180] The movie GATTACA is an example projecting, from current knowledge and technology, a world where the new eugenics is a reality.[181] If researchers are able to access the DNA profiles or DNA samples accumulated pursuant to a DNA database statute, they will inevitably try to identify the genes responsible for particular traits. Thousands of citizens would essentially be contributing to this future reality without their knowledge or consent. This reality is not as far off as some may

175. DNA AND THE CRIMINAL JUSTICE SYSTEM, *supra* note 6, at 177.

176. HUMAN GENETICS COMMISSION, NOTHING TO HIDE, NOTHING TO FEAR?: BALANCING INDIVIDUAL RIGHTS AND THE PUBLIC INTEREST IN THE GOVERNANCE AND USE OF THE NATIONAL DNA DATABASE 74–75 (2009).

177. THE DISABILITY STUDIES READER 17 (Lennard J. Davis ed., 1997).

178. David A. Kirby, *The New Eugenics in Cinema: Genetic Determinism and Gene Therapy in "GATTACA,"* 27 SCIENCE FICTION STUDIES 193, 195 (2000).

179. Kirby, *supra* note 178.

180. *Id.* at 196.

181. *Id.* at 199.

think. President George W. Bush enacted the Newborn Screening Lives Act in April 2008, which mandates the screening of the DNA of all newborn babies in the U.S., and sections of the bill make it clear that the DNA may be retained and later used in genetic experiments and tests.[182] In addition, all 50 states now routinely provide the results of such tests to the Department of Homeland Security.[183] The National Conference of State Legislatures has created a list of the various statutes or regulatory provisions by state under which newborns' DNA is being collected.[184]

IX. Function Creep

State and federal DNA database statutes include no provisions for destroying DNA samples once a DNA profile for inclusion in CODIS has been generated.[185] Proponents of forensic DNA testing claim that retaining DNA samples is necessary because science and technology is constantly improving and these samples may yield more information in the future.[186] Paul Ferrara, Director of Virginia's DNA program, additionally claims that retaining DNA samples is necessary so that agencies can rerun DNA profiles to verify cold hits before notifying law enforcement agencies to further investigate, and that agencies encounter many different situations requiring consultation with original database samples.[187]

The term *function creep* refers to the "operationally driven use of the existing resource for new purposes not envisaged when the resource was established," which is "made possible by technological innovation and lack of inhibiting measures" like public opposition or legislation.[188] Historically, databases that were created in the U.S. for

182. Steve Watson, "Bush Signs Bill to Take All Newborns' DNA," Infowars.net, May 2, 2008, *available at* http://www.infowars.net/articles/may2008/020507DNA.htm.

183. *Id.*

184. National Conference of State Legislatures, Newborn Genetic and Metabolic Disease Screening, *available at* http://www.ncsl.org/IssuesResearch/Health/NewbornGeneticandMetabolicScreeningLaws/tabid/14416/Default.aspx (last visited April 19, 2010).

185. DNA AND THE CRIMINAL JUSTICE SYSTEM, *supra* note 6, at 190.

186. *Id.* at 215.

187. Paul Ferrara, Director, Virginia DNA Program, Proceedings of the National Commission on the Future of DNA Evidence (Jul. 26, 1999).

188. HUMAN GENETICS COMMISSION, NOTHING TO HIDE, NOTHING TO FEAR?: BALANCING INDIVIDUAL RIGHTS AND THE PUBLIC INTEREST IN THE GOVERNANCE AND USE OF THE NATIONAL DNA DATABASE 39 (2009).

a discrete purpose were eventually assigned new functions and purposes.[189]

The government began issuing drivers licenses in the name of public safety, and yet the average adult American citizen now has more direct dealings with government through licensing and regulation of the automobile than through any other single public activity.[190] Eventually, states began earning millions of dollars per year from selling drivers' personal information to direct marketers, charities, political campaigns and various commercial interests.[191] An unintended consequence of this practice was the real threat to public safety. In some instances, abuse of drivers' personal information lead to murders.[192] Congress reacted by passing the Drivers Privacy Protection Act, which effectively prohibits the disclosure of personal information obtained in connection with a motor vehicle record for unauthorized uses unless the individual waives his or her right to privacy.[193] The U.S. Supreme Court upheld the constitutionality of the Drivers Privacy Protection Act, reasoning that it is a proper exercise of Congress' authority to regulate interstate commerce under the Commerce Clause and does not violate principles of federalism contained in the Tenth Amendment.[194]

The government introduced social security numbers (SSNs) to track individuals' accounts within the Social Security Program in 1935.[195] Executive Order 9397, issued in 1943, expanded its use by requiring federal agencies to use SSNs exclusively whenever a new identification system for individuals needed to be created.[196] Eventually, the Internal Revenue Service adopted the SSN as its official taxpayer identification number and the Department of

189. DNA AND THE CRIMINAL JUSTICE SYSTEM, *supra* note 6, at 174.

190. Carl Watner, *The Precursor of National Identification Cards in the U.S.: Drivers Licenses and Vehicle Registration in Historical Perspective*, *available at* http://www.voluntaryist.com/articles/119a.php.

191. Linda Greenhouse, *Justices Uphold Ban on States' Sales of Drivers' License Information*, N.Y. Times, Jan. 13, 2000, *available at* http://www.nytimes.com/2000/01/13/us/justices-uphold-ban-on-states-sales-of-drivers-license-information.html.

192. Electronic Privacy Information Center, The Drivers Privacy Protection Act (DPPA) and the Privacy of Your state Motor Vehicle Record, http://epic.org/privacy/drivers/ (last visited Dec. 1, 2009); 18 U.S.C.A. § 2721 (West 2009).

193. *Id.*

194. *Reno v. Condon*, 528 U.S. 141 (2000).

195. Social Security Online: The Official Website of the U.S. Social Security Administration, Social Security Number Policy Chronology, http://www.socialsecurity.gov/history/ssn/ssnchron.html (last visited Dec. 1, 2009).

196. *Id.*

Defense began using SSNs to identify Armed Forces personnel. [197] Then during the 1970s, the Bank Records and Foreign Transactions Act required all financial institutions to obtain the SSNs of all of their customers, the Privacy Act authorized local governments to use SSNs, and the Tax Reform Act authorized registration authorities of a state or local tax, welfare, driver's license, or motor vehicle registration to use SSNs to establish identities.[198] Finally, in 1987, the Social Security Administration began automatically issuing SSNs to newborns when the birth was registered by the State, and currently all 50 states, plus Washington D.C. and Puerto Rico, participate in this program.[199] Once intended to track individuals' accounts within the Social Security Program, SSNs have become a universal identifier for individuals within the U.S.

The U.S. Constitution expressly states that "an enumeration shall be made within three Years after the first Meeting of the Congress of the United States, and within every subsequent Term of ten Years in such Manner as they shall by Law direct."[200] Census records are a constitutional requirement used to allocate congressional seats, electoral votes and government program funding. Though the Constitution only requires a head count, a substantial amount of data is collected during a census.[201] More and more detailed information has been gathered over the years, including data on race/ancestry, health, housing, and transportation.[202] After the Japanese Attack on Pearl Harbor, census records were used to facilitate the internment of Japanese-Americans.[203] Presently, however, census data cannot be used for any purpose other than its intended statistical purposes, and no federal agency is allowed to access census reports.[204]

The Texas Tribune recently published a story about how the Department of State Health Services in Texas turned over newborn

197. *Id.*

198. *Id.*

199. *Id.*

200. U.S. CONST. art. I, § 2, cl. 3.

201. U.S. Constitution Online, Constitutional Topic: The Census, http://www.usconstitution.net/consttop_cens.html (last visited Dec. 1, 2009).

202. U.S. Census Bureau, History: Index of Questions, http://www.census.gov/history/www/through_the_decades/index_of_questions/ (last visited Dec. 1, 2009).

203. WILLIAM SELTZER & MARGO ANDERSON, AFTER PEARL HARBOR: THE PROPER ROLE OF POPULATION DATA SYSTEMS IN TIME OF WAR 4–22 (2000) (unpublished draft manuscript), *available at* https://pantherfile.uwm.edu/margo/www/govstat/newpaa.pdf.

204. 13 U.S.C.A. § 9 (West 2009).

DNA samples to an Armed Forces lab "to build a national and, someday, international mitochondrial DNA registry."[205] However, the newborn blood samples were stored without parental consent and records uncovered government efforts to limit the public's knowledge of the state newborn blood program.[206] Parents sued officials over these actions, but the state settled the case quickly before anything could be revealed in the discovery phase.[207]

As of 2004, the Department of Defense ("DOD") had collected three million biological samples from service personnel "for the stated purpose of identifying remains or body parts of a soldier killed on duty."[208] However, samples are retained for fifty years, which greatly exceeds the subjects' time with the military. Further compounding the issue, the DOD has refused to establish regulations to guard against third parties accessing the accumulated biological samples.[209] It is not hard to foresee pressures mounting to use these biological samples for purposes other than identifying soldiers killed on duty, such as identifying criminal suspects and medical research.[210]

Although there is a Fourth Amendment concern associated with obtaining DNA samples, the Fourth Amendment applies only to government action and is inapplicable to private parties who do not act as agents of the government.[211] This doctrine, however, does not preclude the possibility that law enforcement may be able to access existing repositories of DNA from cooperative private hospitals or laboratories, provided that the government had no involvement in how the DNA was originally obtained and that the state is not engaging in any search or seizure in acquiring DNA in this way.[212] The National Bioethics Advisory Commission estimated that as of 1998, more than 282 million human biological specimens were collected and stored in the U.S. for research studies, newborn screening tests, organ banks, blood banks, forensic DNA databases, and for other purposes, which increases at a rate of 20 million samples

205. Emily Ramshaw, "DNA Deception," The Texas Tribune, Feb. 22, 2010, *available at* http://www.texastribune.org/stories/2010/feb/22/dna-deception/.

206. *Id.*

207. *Id.*

208. DNA AND THE CRIMINAL JUSTICE SYSTEM, *supra* note 6, at 175.

209. *Id.*

210. DNA AND THE CRIMINAL JUSTICE SYSTEM, *supra* note 6, at 175.

211. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

212. Edward J. Imwinkelried & D.H. Kaye, *DNA Typing: Emerging or Neglected Issues*, 76 Wash. L. Rev. 413, 425 (2001).

per year.[213] The issue lies in the fact that an individual undergoing diagnostic tests or donating samples for clinical or research purposes has a reasonable expectation of privacy that their test results and DNA will not be shared with a non-medical third party without his or her consent.[214]

Function creep has already begun with DNA databases as law enforcement has expanded DNA collection to include new categories of people.[215] Examples of future uses of DNA databases include research to increase understanding of patterns of criminal behavior, research to correlate genetic variation with disposition to certain behaviors, and creation of a universal database by combining all existing databases to facilitate data sharing.[216]

X. Conclusion

DNA database statutes provide inadequate privacy protections. There is a lack of national oversight, no uniform quality control process of obtaining DNA samples and maintaining DNA databases, and there is no consistency regarding who may access DNA databases and for what reasons. DNA is a useful crime-fighting tool, but its potential makes it likely to be abused. Because DNA databases already exist, it is hard to imagine that their viability will diminish in the future. Therefore, leaders must work to ensure that all DNA profiles and DNA samples are used for the limited purpose for which they were collected, and advocates should push for the eventual destruction of all DNA samples once DNA profiles have been generated so that no one will be tempted to use them for purposes that go beyond forensic identification.

The way cold hit statistics are used to determine guilt or innocence in litigation is another area of potential abuse. Increasingly, convictions are relying on DNA evidence alone. Moreover, when the DNA evidence is a partial match on less than 13 loci, the risk of injustice is greater, as evidenced by the report of Arizona's DNA database in 2005. It is frightening that most people are blinded by a belief that DNA is the panacea of crime detection

213. NATIONAL BIOETHICS ADVISORY COMMISSION, RESEARCH INVOLVING HUMAN BIOLOGICAL MATERIALS: ETHICAL ISSUES AND POLICY GUIDANCE 13 (1999).

214. *See* Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001).

215. DNA AND THE CRIMINAL JUSTICE SYSTEM, *supra* note 6, at 174.

216. HUMAN GENETICS COMMISSION, NOTHING TO HIDE, NOTHING TO FEAR?: BALANCING INDIVIDUAL RIGHTS AND THE PUBLIC INTEREST IN THE GOVERNANCE AND USE OF THE NATIONAL DNA DATABASE 81–85 (2009).

and do not recognize the potential threat to privacy and other civil liberties. Researchers should be provided with access to the genetic profiles within CODIS after all of the personal identifiers have been removed so that they can conduct independent scientific scrutiny to ensure the scientific integrity of DNA forensic science.

The NDNAD in the UK is even more controversial than the DNA databases in the U.S. Despite negative media coverage and successful legal challenges to DNA collection and retention practices, British leaders are forging ahead with the hope of one day expanding the database to cover the entire UK population.

Given the history of eugenics and discrimination in the U.S. and abroad and the atrocities that have befallen millions of innocent human beings, everyone should be aware of and fear the dangers associated with becoming a genetic surveillance society. If people are not vocal in opposing current DNA database practices, the only people who will be shaping the future of how DNA is used are those with a political agenda who are not as concerned with individual privacy and the ethics of their actions. As science and technology continue to advance, visions of a brave new world that are the substance of science fiction movies like GATTACA may no longer be a distant reality.

***